NISTIR 4781

Privacy Protection in the United States

A 1991 Survey of Laws and Regulations Affecting Privacy in the Public and Private Sector Including a List of All Relevant Officials

Prepared by Ronald L. Plesser and Emilio W. Cividanes of Piper and Marbury

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Barbara Hackman Franklin, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4781

Privacy Protection in the United States

A 1991 Survey of Laws and Regulations Affecting Privacy in the Public and Private Sector Including a List of All Relevant Officials

Prepared by Ronald L. Plesser and Emilio W. Dividanes of Piper and Marbury

Edward Roback
NIST Coordinator

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

February 1992

U.S. DEPARTMENT OF COMMERCE
Barbara Hackman Franklin, Secretary

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

Preface

This National Institute of Standards and Technology Interagency Report (NISTIR) presents a survey of laws and regulations affecting privacy in the public and private sectors prepared by Mr. Ronald L. Plesser and Mr. Emilio W. Cividanes of Piper & Marbury. This survey may be particularly useful to federal agencies when planning or evaluating the privacy and security of automated information system assets.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this material. However, as this material may be of use to federal organizations, it is being reprinted by NIST to provide for governmentwide dissemination of this work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to Mr. Ronald L. Plesser, Mr. Emilio W. Cividanes, and Piper & Marbury for their kind permission to publish this material.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

PRIVACY PROTECTION IN THE UNITED STATES

A 1991 Survey of Laws and Regulations Affecting Privacy in the Public and Private Sector Including a List of All Relevant Officials

Prepared By:

Ronald L. Plesser
Emilio W. Cividanes
Piper & Marbury
1200 19th Street, N.W.
Washington, D.C. 20036

May 1991

PRIVACY PROTECTION IN THE UNITED STATES

PRIVACY PROTECTION IN THE UNITED STATES

INTRODUCTION

Data protection laws have existed in various European countries for more than a decade. Their goal is the protection of personal record privacy without unduly constraining legitimate uses of personal data, including the cross-border flows of such data. There is also a well-developed history of privacy protection in the United States.

The Commission of the European Communities' ("EC") proposal for a directive (SYN 287) of September 13, 1990 on the confidential treatment of personal data has refocused attention on the issues of personal record privacy and data protection. The Organization for Economic Cooperation and Development ("OECD") and the Council of Europe are also actively examining the issues of privacy and data protection. As a result of these activities, countries without data protection laws may have to adopt such laws for the first time. Countries with current laws may also need to adopt amendments to bring their laws into conformity with the principles and requirements of the EC directive. Moreover, the laws and practices of countries like the United States probably will be examined in relation to those of other countries to determine whether they are "adequate" for the purpose of using personal data obtained from countries with data protection requirements.

A similar examination of United States laws last occurred in the early 1980s when the OECD adopted "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" and the Council of Europe presented a Data Protection Convention. In 1982 the National Telecommunications and Information Administration ("NTIA") of the U.S. Department of Commerce issued an excellent report entitled "Privacy Protection Law in the United States." That report examined U.S. privacy laws grouped according to the principles of the OECD guidelines. The NTIA report concluded that:

> The body of law implementing privacy protection principles in the United States has evolved in diverse, multi-jurisdictional layers, reflecting our pragmatic, pluralistic system as well as an inclination to avoid centralized authority over personal data. Much of the law is rooted in Constitutional restrictions on the power of government, and in the individual's common-law "right to be let alone." In some areas, the source of protection is the Federal Congress and courts; however, the States have also acted to protect privacy in the many areas where they have traditionally asserted jurisdiction. As a result of the broad range of concerns covered by modern definitions of privacy, and the pragmatism that has informed the application of privacy principles, the content of privacy law varies widely for different kinds of record-keeping activity, with more comprehensive coverage of the government than of the private sector. The end result is a highly varied system of privacy law which nevertheless affords an extensive network of protections for the individual.

This report updates that earlier NTIA analysis and is divided into six parts: this essay and five appendices. Appendix 1 lists in alphabetical order and briefly describes

most of the current federal and state laws protecting personal information privacy. Appendix 2 groups these laws according to the general principles of data protection as reflected in the EC directive. Appendix 3 reflects in a tabular form Appendix 2's grouping of federal laws. Appendix 4 lists the agencies responsible for enforcing federal privacy laws. Appendix 5 reproduces the text of the 1982 NTIA report (without the report's supplementary appendices).

The analysis in this report is intended to reflect many of the changes and advances in U.S. privacy law since 1982. It does not attempt to qualitatively compare U.S. privacy law with the European data protection approach. The reason is that the two approaches are quite different and not really comparable. The European approach follows an administrative approach to the regulation of electronic data bases and files. Private sector and public sector records are all subject to one unifying set of principles and requirements. European data protection laws are aimed primarily at the government protecting the individual from the private sector. They are omnibus in the ubiquitousness of their requirements.

In contrast, privacy stands in the U.S. as only one of very few exceptions to the free flow of information. The First Amendment of the U.S. Constitution and the Freedom of Information Act, and their state counterparts, as well as the

limited scope of protections afforded by the Copyright Act of 1976 (and its constitutional foundation and common law counterparts), illustrate the tendency in U.S. law to favor and facilitate the flow of information, free from governmental control. Furthermore, U.S. privacy law aims primarily at protecting individuals from abuses by government, while also protecting in a very targeted or sectorial manner against abuses by custodians of private-sector records.

Moreover, a hallmark of U.S. privacy law is its diversity. The two key diversifying influences are (1) the law's long history of development and (2) our nation's decentralized, federalist system of government which encourages local experimentation and favors state-sponsored solutions. This has resulted in a dispersion of authority to make, interpret, and apply privacy law. See generally Appendix 4.

For example, the two-hundred year-old U.S. Constitution (most of its safeguards which apply to the states) demarcates a zone of privacy around the individual by restricting the means by which Government can collect information about individuals and the uses which it can make of such information (see Fourth Amendment restrictions and First Amendment and Equal Protection clause protections). It also ensures procedural fairness by requiring that individuals be given a fair opportunity to challenge adverse governmental

actions against them and scrutinize the factual records upon which they have been based (see Due Process clause safeguards).

Privacy safeguards are also found in the "common law," a body of legal rules which originated in historical usages and customs in the British laws given recognition by early U.S. courts, and which is continuously evolving through judicial interpretation. Common-law rules, for example, limit intrusive collection of personal information, penalize unwarranted disclosure of such data, and protect against disclosure of erroneous data about individuals. Responsibility for interpreting and applying these rules lies primarily with state courts.

Statutory law has played an increasingly important role during the past twenty years in the development of U.S. privacy law. These statutes often build upon existing common-law rules -- clarifying, redefining, and sometimes creating new rights -- rather than supplanting them, and often also are influenced by constitutional principles. Statutory law and related regulations are primarily responsible for developing the interests of individuals to learn the contents of records about them and to participate in setting conditions for their use.

This centuries-old tradition of diversity and dispersion of authority has facilitated flexible responses by courts and legislatures to privacy-based concerns and abuses.

It also has left to the states the authority to protect the privacy of state records, thereby precluding any one federal statute from having jurisdiction over all records in the U.S. Consequently, the U.S. does not have a single, omnibus data protection law that covers both public and private sector records, nor one law that covers all forms of data collection by governmental records. Nor does it have a central privacy or data protection commission, or a single regulatory body that oversees data protection. Nevertheless, the hundreds of federal and state laws, supported by self-regulatory activities, provide an extensive network of privacy protection.

Indeed, the U.S. Privacy Protection Study Commission -- an independent body established by federal law to study the practices "in force for the protection of personal information" -- explicitly rejected in 1977 a proposal for an omnibus privacy statute establishing governmental authority to regulate the flow of all personal data. Its rejection was based on several considerations, including: (1) the danger of government control over the flow of both public and private information; (2) the greater influence on the private sector than on the public sector of economic incentives that encourage voluntary compliance with privacy principles; and (3) the difficulty of legislating a single standard for widely varying record-keeping practices in the private sector.

The standards applied to the various record-keeping relationships in the private sector have emerged from sharply focused legislative inquiries that identify problems arising in particular record-keeping relationships. By considering the distinct role that the specific type of records play in the lives of individuals, and the nature of the harm caused by their misuse, Congress and state legislatures have been able to balance the privacy interests at stake against the public interests served by using personal data in the various contexts. As noted above, the statutes that have emerged from this process have been heavily influenced by constitutional principles and other legal rules.

I. FUNDAMENTAL PRINCIPLES OF U.S. PRIVACY PROTECTION POLICY

In 1977, the Privacy Protection Study Commission reported its findings to the U.S. Congress and recommended ways of providing additional protection for the privacy of individuals while meeting society's legitimate needs for information. The Commission based its recommendations on the conclusion that effective privacy protection must have three concurrent objectives:

- minimize intrusiveness in the lives of individuals;
- maximize fairness in institutional decisions made about individuals; and
- provide individuals with legitimate, enforceable expectations of confidentiality.

U.S. privacy laws generally contain provisions advancing these objectives. The 1982 NTIA report identified many of the U.S. federal and state laws that seek to accomplish these objectives by, for example, creating a proper balance between what individuals are expected to divulge to record-keeping organizations and what these individuals seek in return; by opening up record-keeping operations in ways that will minimize the extent to which recorded information about individuals is itself a source of unfairness in any decisions made about them on the basis of the information; and by creating and defining obligations with respect to the uses and disclosures that are to be made of recorded information about individuals.

II. DEVELOPMENTS IN U.S. PRIVACY LAW SINCE 1982

Since the issuance of the 1982 NTIA report there have been several important advances in U.S. privacy laws. On the federal level these have by and large responded to technological changes of computers, digitized networks, and the creation of new information products. This essay examines some of these advances, particularly three federal privacy statutes all related to the development of greater privacy protection of personal records maintained by non-governmental agencies. These three, all enacted in response to new technological developments in the delivery and marketing of information, are: (i) the subscriber privacy provisions of the Cable

Communications Policy Act of 1984; (ii) the Electronic Communications Privacy Act of 1986; and (iii) the Video Privacy Protection Act of 1988. The common threads of these three statutes is that they all respond to new technologies, protect against government access to private records, and prohibit anyone's unauthorized use of the collected information.

Cable Communications Policy Act of 1984

Congressional concern with evolving cable television technology capable of intrusive data collection led to the enactment of the subscriber privacy provisions of the Cable Communications Policy Act of 1984. The technology Congress sought to protect against was the ability of cable operators to monitor subscriber viewing habits, as well as subscriber banking, shopping, and other personal transactions that might occur over a "two-way", interactive cable system. This technology threatened an individual's ability to keep his or her viewing habits and transactions confidential. The law thus established a careful scheme of notice and consent which permits cable television subscribers to know what a cable operator's practices are and provides them the opportunity to limit the data collections and disclosures that their cable operator may make.

The Cable Act thus requires cable television operators to inform their subscribers at the time of entering into a contractual arrangement, and annually thereafter, about the

nature of the personal data they collect about subscribers, their data disclosure practices, and subscriber rights to inspect and correct errors in such data. The law also prohibits a cable operator from using the cable system to collect information about its subscribers without their consent, and generally bars disclosure of such data. It provides for law suits for enforcement of these rights and authorizes awards of compensatory damages, punitive damages, costs, and attorneys' fees against cable operators that violate the Act's privacy provisions.

A cable operator may rent mailing lists for purposes unrelated to cable service after notifying subscribers of such possibility. Subscribers have the absolute right to prohibit the inclusion of their name on such a mailing list. This approach carries forward the market practice known as a "negative option" which infers customer consent where a customer has been notified of his or her right to object to the disclosure and he or she has chosen not to exercise that right. A recent nationwide poll found that an overwhelming majority of Americans support the "negative option" approach to protecting consumer privacy. See The Equifax Report on Consumers in the Information Age: A National Opinion Survey (1990). This approach also reflects the principle that whenever possible, information collected for one purpose should

not be used for another purpose without the individual's consent.

In addition, consistent with the traditional U.S. concern with governmental abuses, the law prohibits governmental entities from obtaining personal subscriber data collected by a cable operator without a court order reflecting a judicial finding that the data sought is likely to reveal criminal activity. Subscribers must be notified of the government's request and provided with an opportunity to contest the government's claims prior to a court decision.

While the U.S. cable television industry has not evolved into the highly intrusive, "two-way" interactive presence that Congress believed it would, the law has been applied to cable television companies operating "one-way," noninteractive systems. See, e.g., Warner v. American CableVision of Kansas City, 699 F. Supp. 851 (D.Kan. 1988), remanded with instructions to vacate, slip op., No. 1880-2820 (10th Cir. Jan. 6, 1989). Moreover, the law's provisions have served as a model for other federal and state privacy legislation. See, e.g., Video Privacy Act, codified at 18 U.S.C. § 2710.

Electronic Communications Privacy Act of 1986

Congressional concern with technological advances that had made the 1968 wiretap statute obsolete led to the enactment of the Electronic Communications Privacy Act ("ECPA"). The

1968 law protecting the privacy of users of telephone services had been passed prior to major advances in computer technology and the growing use of telephone systems for electronic mail and other computer-to-computer data transmissions. The law prohibits the interception of wire and oral communications without a warrant or court order. As a result, it is illegal in the United States to listen into a telephone call or to eavesdrop.

Congress sought through ECPA to extend the telephone network privacy safeguards codified in the 1968 law to the new technology, including microwave transmission of telephonic communications and non-network data banks of electronic messages.

ECPA accomplished its goals by various means. For example, the law extended the prohibition against unauthorized interception of "wire" telephone conversations to cellular. While the prohibition applies to the public and private sectors alike, governmental entities may seek judicial approval for intercepting such communications by way of a court-issued search warrant if they show that probable cause exists to believe that the sought-after conversations will reveal evidence of criminal conduct. Violations of the prohibition may result in criminal prosecution, fines, and imprisonment, and/or civil liability of not less than $100 for each day of violation. In addition, an individual can suppress the use as

evidence of data the government collected through an illegal interception.

However, ECPA has two other provisions of particular interest here because they concern stored data. First, ECPA's stored communications provisions extend to customer toll records -- records that identify the calls placed from a telephone and are collected for billing purposes -- protections similar to those afforded to cable television subscriber records. That is, the new law prohibits governmental entities from obtaining toll records without a court order reflecting a judicial finding that the data sought is likely to reveal criminal activity. Customers must be notified of the government's request and provided with an opportunity to challenge the government's access.

Second, ECPA's stored communications provisions also prohibit the unauthorized access to or use of stored electronic communications such as "voice mail," electronic mail, and other types of computer-to-computer communications. These communications are in many ways the electronic counterparts to letters, memoranda, or files transported via the postal system. ECPA addresses the problem of persons gaining unauthorized access -- or exceeding their authorized access -- to those electronic communications that, like personal or business correspondence, are intended to be kept confidential. Violations of these provisions can result in imprisonment and

fines of up to $250,000, and/or civil liability for damages suffered and profits made by a violation.

Video Privacy Protection Act of 1988

Enactment of the Video Privacy Protection Act resulted from congressional concern that some of the same problems that threatened the privacy of cable television subscribers prior to passage of the 1984 Cable Act now threatened the privacy of the large segment of the American public that uses video cassettes for educational and entertainment purposes. Treating transactions involving videos much as most states treat records that libraries maintain about patrons borrowing books (see Fair Information Practices Statutes), Congress sought to guard against forms of surveillance that result in individuals being chilled in their social and educational experimentation with ideas. Protecting an individual's choice of books and films has long been a pillar of the intellectual freedom Americans enjoy by virtue of the first amendment to the U.S. Constitution. Congress thus set out to protect individuals against public and private surveillance of the trail of information generated by purchases and rentals of video-cassettes and other audiovisual materials.

The law prohibits video service providers from disclosing to anybody information that links customers to particular materials or services without customer consent, except in certain limited circumstances. For example, the Act

prohibits law enforcement agencies from obtaining personally identifiable information maintained by video providers without a court order reflecting a judicial finding that there is probable cause to believe that the data sought is relevant to a legitimate law enforcement inquiry. Such court orders may be issued only with prior notice to the consumer whose personal data is sought.

The law does permit a video service provider to release customer mailing lists provided that the lists do not disclose the customers' actual selections and that the video provider has furnished consumers with the opportunity to prohibit such disclosure. This is the "opt out" practice referred to earlier.

The Act authorizes awards of damages, punitive damages, costs, and attorneys' fees for individuals whose personal data has been unlawfully disclosed.

Two other legislative measures are worth discussing briefly. They are the Polygraph Protection Act of 1988 and the Computer Matching and Privacy Protection Act of 1988.

Polygraph Protection Act of 1988

Another significant development during the 1980s was national legislation abolishing the private sector's use of the polygraph machine. Although the 1988 federal law permits governments and law enforcement agencies to continue using these "lie detector" machines, they may do so only subject to

safeguards, including the constitutional due process protection that applies to governmental use of the results of polygraph tests.

While the elimination of polygraph testing in the private sector has not necessarily been viewed as a data protection or privacy law, it is very significant in that the law protects against the unfair use of unreliable information by prohibiting its collection. The law advances all three fundamental goals of U.S. privacy protection policy. It protects against a method of data collection which is inherently intrusive because persons subjected to polygraph testing cannot control the questions that are asked of them nor their responses. By precluding the use or consideration of information collected by means of inherently unreliable technology, the law promotes fairness in institutional decisionmaking. And, by creating specific rights and penalties, the law provides individuals with legitimate, enforceable expectations of confidentiality. The federal polygraph ban also is significant because it is not aimed at any specific sector of society but rather impacts all non-governmental sectors equally. In this way, the law is atypical of U.S. privacy laws that affect the private sector.

Computer Matching and Privacy Protection Act of 1988

An additional significant change in privacy law applies only to federal records. The Computer Matching and

Privacy Protection Act of 1988 for the first time set rules regulating how federal agencies may match personal information held in their data bases with data stored in other data bases. Computerized matching is the computerized comparison of two data bases to look for the same record in both systems, usually for the purpose of identifying individuals who may be defrauding the government. For example, a government agency may "match" its employee list with a list of persons receiving public assistance. This would identify persons who were earning an income and improperly receiving public assistance at the same time. Such matching, without regulation, can result in indiscriminate swapping of data files. While the 1974 Privacy Act was designed to prevent the unconsented use of personal data for a purpose different than for what it was collected, misapplication of the law's "routine use" exception -- permitting unconsented disclosures for purposes compatible but not identical with the reason for the data file's creation -- resulted in widespread computer matching by federal agencies.

The 1988 statute does not close the loophole created by the "routine use" exception. Matching continues to be included in the category of "routine use" of personal records held by federal agencies. However, the Act requires agencies, before conducting a match, to enter into written agreements specifying the purpose of the match, the records to be matched, and a cost/benefit analysis of the match. It also prohibits

agencies from taking any adverse action against an individual based on a match until the results have been independently verified. The statute also establishes Data Integrity Boards within each department and agency to oversee the internal and external matching programs.

The Act thus creates an important procedural framework of more adequate notice to individuals, the right to a hearing before government benefits are cut off or denied, and mandatory reporting requirements for agencies that match records.

III. FEDERAL PRIVACY GUIDELINES AND INDUSTRY SELF-REGULATION

In August 1990, after many months of study and consultation, President Bush's Special Adviser for Consumer Affairs issued voluntary guidelines for the use and distribution of personal information generated by consumer use of services accessed by telephone, such as electronic data bases, audiotex, and videotex. The guidelines also were spurred by changing consumer practices brought about by technological advances.

The guidelines were based on the following general privacy protection principles which the Special Adviser urged all industries to apply in their operations:

1. Tell consumers, in language they can understand, when and why certain information is being collected, what's going to be done with it, and who will have access to it. Tell them how you plan to protect their privacy, and ask for their feedback on your policy.

2. Collect only that information which is germane to the transaction at hand. And do not allow the information to be used or sold for other

incompatible purposes without the individual's knowledge.

3. Provide consumers a copy of their files upon request, and make it easy for them to correct errors and include statements of explanation.

4. Allow consumers to opt out of direct marketing or other uses they feel are inappropriate for the information they are providing.

5. Make a concerted effort to educate consumers generally about how information about them is gathered, analyzed, grouped into lists and rented or sold, or otherwise used.

The Special Adviser's principles reflect sound business practices that generate customer good will by protecting consumer privacy while identifying circumstances where, absent objection, industry can still use some personal data to better serve the consumer. As the principles become the basis for future ethical codes adopted by some private sector industries, they can already be seen embodied in some existing codes. For example, the Guidelines for Personal Information Protection and Guidelines for Mailing List Practices adopted by the Direct Marketing Association ("DMA") already reflect the Special Adviser's principles. The DMA is a trade association of companies that utilize direct response advertising methods to market goods and services. Members of DMA encompass all aspects of the American business community. Virtually all big businesses, responding to social change and the growing sophistication of technology and its decline in cost, use direct response as a part of their marketing

strategy. Major companies with large direct response programs include Sears and Roebuck, American Express, Merrill Lynch, General Mills, IBM, Xerox, and major automobile manufacturers such as BMW and Toyota.

The DMA guidelines provide for the Mail Preference Service ("MPS") name removal file. DMA's MPS name removal file was established in 1971 in response to consumer requests to control their mail volume. A companion service, the Telephone Preference Service ("TPS") was established in January, 1985, as an answer to increased consumer inquiries regarding telephone marketing. A consumer by contacting the DMA can have his or her name placed on the MPS or TPS. Marketers use this list to eliminate such consumers from mailings or telephone campaigns.

In 1977, the U.S. Privacy Protection Study Commission recognized MPS as an alternative to legislation regarding mailing list usage. The Commission also encouraged individual direct marketers to give people on lists an opportunity to indicate they do not wish their names made available to outside sources for marketing purposes. DMA supported this effort in its "Freedom To Mail" campaign and sought to expand the existence of in-house mail preference or "opt out" programs.

As a result, many direct marketers established in-house mail preference services, or suppression files so that consumers could enjoy the convenience of shopping by mail, while at the same time controlling their mail volume.

Telephone marketers are also encouraged to use in-house suppression as a means of ensuring that solicitation calls are only targeted to those who are most receptive.

The in-house suppression program adopts a policy of notification and ability to opt-out. Typically, a catalog company or credit grantor will inform its customers that it may make its mailing list available to others. Industry support of the service shows a commitment to self-regulation, thereby improving the consumer's acceptance of direct marketing. MPS and TPS are also seen as a means to save valuable marketing dollars by deleting unresponsive consumers from lists.

CONCLUSION

The United States provides a highly varied privacy protection system that affords individuals with an extensive network of protections. Its strength is its ability to evolve and respond to changes. For example, by repeatedly taking steps to protect individuals from new threats to their privacy, the U.S. system has shown its ability to respond to technological advances. Specifically, in addition to the privacy protection measures adopted by the federal government during the 1980s, including the measures described in this essay, state governments during that same time adopted approximately 200 additional privacy laws. If the past is indeed prologue to the future, then the U.S. privacy protection system will continue to evolve and respond to new privacy challenges as they arise.

APPENDIX 1

GLOSSARY OF UNITED STATES PRIVACY LAWS

This list describes Federal and State laws protecting against abuse in the collection or use of personal data. While these legal protections are listed in Appendix 2 according to categories which reflect principles underlying the personal data directive of the Council of the European Community, they are listed here only according to their Federal or State origin.

Federal statutes are cited by reference to the United States Code (U.S.C.). State law generally is cited by reference to State codes. In some instances, State law is cited by example --- statutes in a particular State which illustrate a proposition about the law of many or most States. Professor Prosser's well-known treatise Law of Torts is cited in support of certain common law rules.

This list was prepared by the law firm of Piper & Marbury.

FEDERAL CONSTITUTION PROVISIONS

First Amendment - Restricts governmental inquiries into an individual's political and religious beliefs and affiliations.

Fourth Amendment - States: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath and affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Courts have interpreted the amendment to restrict the means used by the government to collect information from places in which an individual has a reasonable expectation of freedom from governmental intrusion. It places limits, for example, on wiretapping, electronic eavesdropping, access to electronic mail and other computerized records, and the opening of mail by government agencies.

Fifth Amendment - States in part that "[N]o person . . . shall be compelled in any criminal case to be a witness against himself." This provision limits the means used by government to collect incriminating information from an individual in a variety of contexts -- from custodial police interrogations to

the filing of tax returns -- in addition to limiting the scope of questioning in criminal proceedings themselves.

The Fifth Amendment also prohibits the Federal government from depriving a person of "life, liberty, or property" without "due process of law." Requires procedures designed to ensure that the individual has a reasonable opportunity to challenge any proposed governmental deprivation. At a minimum, there must be notice and a hearing at which the factual basis of the decision is subject to scrutiny.

By implication, the Fifth Amendment also severely limits Federal government use of "suspect" personal characteristics to adversely classify or penalize individuals. Classifications based on race or national origin are especially suspect and require "strict" judicial scrutiny. Also suspect, but subject to less exacting scrutiny, are classifications based on sex and place of citizenship.

Fourteenth Amendment - The fundamental amendment to the U.S. Constitution that applies the First, Fourth, and Fifth Amendments to the states. Prohibits state and local governments from depriving a person of "life, liberty, or property" without "due process of law." Requires procedures designed to ensure that the individual has a reasonable opportunity to challenge any proposed deprivation. At a minimum, there must be notice and a hearing at which the factual basis of the decision is subject to scrutiny.

The equal protection clause severely limits state and local government use of "suspect" personal characteristics to adversely classify or penalize individuals. Classifications based on race or national original are especially suspect and require "strict" judicial scrutiny. Also suspect, but subject to less exacting scrutiny, are classifications based on sex and place of citizenship.

FEDERAL STATUTES

Administrative Procedure Act (5 U.S.C. §§ 551, 554-558) - Establishes detailed procedures for Federal agencies to follow during administrative hearings. The Act's provisions prescribe, for example, the means by which agencies must notify individuals of their rights and liabilities, and how agencies may collect, present, and evaluate evidence and other data in such hearings.

Cable Communications Policy Act (47 U.S.C. § 551) - Requires cable television operators to inform their subscribers annually about the nature of personal data collected, data disclosure

practices, and subscriber rights to inspect and correct errors in such data. Prohibits a cable television company from using the cable system to collect personal information about its subscribers without their prior consent, and generally bars the cable operator from disclosing such data. Authorizes damage awards of at least $1,000, and awards of punitive damages, costs, and attorneys fees against cable television companies that violate the Act's subscriber privacy provisions.

Also prohibits a governmental entity from obtaining personal subscriber data in a cable television company's possession absent a court order reflecting a judicial finding that the data sought is likely to reveal criminal activity. Subscribers must be notified and provided with an opportunity to contest the government's claims.

Census Confidentiality Statute (13 U.S.C. § 9) - Prohibits any use of census data for other than the original statistical purpose. It also prohibits any disclosure of census data that would allow an individual to be identified, except to sworn officers and employees of the Census Bureau. 13 U.S.C. § 9.

Computer Security Act (Public Law 100-235 § 5) - To protect data maintained in government computers, requires each Federal agency to provide mandatory training in computer security awareness.

Criminal Justice Information Systems (42 U.S.C. § 3789g) - Requires that Federally-funded State and local criminal justice information systems include information on the disposition of any arrest. Permits individuals to see, copy, and correct information about themselves in the system.

Drug and Alcoholism Abuse Confidentiality Statutes (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3) - Prohibits disclosure of information collected for federally-funded research and treatment of drug abuse and alcoholism. It also prohibits use of this information for any purpose outside of the research or treatment program, except in cases of medical emergency or where a court order has been issued. Such information is specifically protected from use against the subject of any criminal proceeding. Violators of this statute are subject to a fine.

Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.) - Prohibits persons from tampering with computers or accessing certain computerized records without authorization. The Act also prohibits providers of electronic communications services from disclosing the contents of stored communications. Usually requires that the customer be notified and given an opportunity to contest in court a government entity's request for access to electronic mail or other stored

communications in the control of a provider of electronic communications services or remote computing services.

Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m) - Requires banks to make extensive disclosures to customers about specific electronic funds transfer (EFT) transactions, both at the time the transactions are made and in the form of periodic statements. Requires banks to notify customers, at the time they contract for EFT services, of their rights, liabilities, charges, procedures, etc., connected with the services, and of whom to contact if an unauthorized transfer is suspected. In the case of preauthorized periodic transfers -- such as automatic bill paying -- the bank must provide either positive or negative notice as to whether payments are being made on schedule. Mandates detailed procedures for the resolution of any inaccuracies in customer accounts, and imposes liability on the bank for errors in the transmission or documentation of transfers. An individual who prevails in a civil action for a violation of the Act may recover actual damages sustained, a penalty of $100 to $1,000, attorney's fees and court costs, and in limited situations, treble damages. Criminal penalties may be imposed for deliberate violations of the Act. Numerous federal agencies also have administrative responsibility for enforcing the provisions of this Act.

Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.) - Prohibits employers from requiring a polygraph test as a condition of employment or using the results of such tests as the sole basis for disciplining employees or taking other adverse employment actions. Bars employers from publicly disclosing the results of polygraph tests unless disclosure is made to the government pursuant to a court order or for the purpose of providing the government with information on criminal conduct. Employers that violate the Act may be subject to a fine of up to $10,000, injunctive relief such as employee reinstatements, and awards of damages, costs, and attorneys fees.

Employee Retirement Income Security Act (29 U.S.C. § 1025) - Requires employers to provide employees with access to information about their accrued retirement benefits.

Equal Credit Opportunity Act (15 U.S.C. § 1691, et seq.) - Restricts inquiries into a credit applicant's sex, race, color, religion, or marital status. Prohibits the retention and preservation of certain information by creditors and requires the preservation of certain specified records relating to credit transactions. Regulates the manner in which information collected by creditors may be used in making decisions regarding the extension of credit. Requires that, when credit is denied or revoked, the applicant must be either notified of the reasons for the decision or informed of his right to learn the reasons. In suits brought for violations of the Equal

Credit Opportunity Act, successful plaintiffs may recover actual damages, punitive damages, attorney's fees, and court costs. Individual or class action suits may be maintained for administrative, injunctive, or declaratory relief. Numerous Federal agencies also have enforcement responsibility for the provisions of this Act.

Equal Employment Opportunity Act (42 U.S.C. § 2000e, et seq.) - Restricts collection and use of information that would result in employment discrimination on the basis of race, sex, religion, national origin, and a variety of other characteristics. 42 U.S.C. § 2000e, et seq.

Fair Credit Billing Act (15 U.S.C. §1666) - Requires creditors, at the request of individual consumers, to investigate alleged billing errors and to provide documentary evidence of the individual's indebtedness. Prohibits creditors from taking action against individuals with respect to disputed debts while disputes are under investigation. Any creditor who fails to disclose required information is subject to a civil suit, with a minimum penalty of $100 and a maximum penalty of $1,000 on any individual credit transaction. The Act also imposes criminal liability on any person who knowingly and willfully gives false or inaccurate information, fails to disclose required information, or otherwise violates any requirement imposed by the Act. Any such person is subject to a fine of $5,000 and/or imprisonment for not more than one year.

Fair Credit Reporting Act (15 U.S.C. §§ 1681 et seq.) - Regulates the collection and use of personal data by credit reporting agencies. Requires that when a data broker is hired to prepare an "investigative consumer report" (an investigation into the consumer's "character, general reputation, personal characteristics, or mode of living" by means of interviews with friends, neighbors, and associates), the request for information must be disclosed to the subject of the report, who is then entitled to learn the nature and scope of the inquiry requested. Requires that, if a consumer report is used in any decision to deny credit, insurance, or employment, the report user must tell the consumer the name and address of the reporting agency.

Prohibits disclosure of consumer reports maintained by consumer reporting agencies without consent unless such disclosure is made for a legitimate business purpose or pursuant to a court order.

Requires reporting agencies to use procedures that will avoid reporting specified categories of obsolete information and to verify information in investigative consumer reports that are used more than once. Requires brokers to maintain security procedures, including procedures to verify

the identity and stated purposes of recipients of consumer reports. 15 U.S.C. § 1681, et seq.

Individuals may sue credit reporting agencies or parties who obtain consumer reports for violations of the Act. Individuals may recover for actual damages suffered, as well as attorney's fees and court costs. Punitive damages or criminal penalties may also be imposed for willful violations of the Act. The Federal Trade Commission and other federal agencies responsible for enforcing the provisions of this Act are also empowered to declare actions to be in violation of the applicable statute, issue cease and desist orders, and impose statutory penalties for noncompliance with agency orders.

Fair Debt Collection Practices Act (15 U.S.C. § 1692, et seq.) - Limits the communications that debt collection agencies may make about the debtors whose accounts they are attempting to collect. Imposes liability on debt collectors for any actual damages sustained, as well as additional damages not to exceed $1,000, court costs, and attorney's fees. Numerous federal agencies also have administrative responsibility for enforcing the provisions of this Act.

Fair Housing Statute (42 U.S.C. §§ 3604, 3605) - Restricts the collection and use of information that would result in housing discrimination on the basis of race, sex, religion, national origin and a variety of other factors.

Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) - Permits a student or the parent of a minor student to inspect and challenge the accuracy and completeness of educational records which concern the student. Prohibits schools receiving public funds from using or disclosing the contents of a student's records without the consent of the student or of the parent of a minor student. Prohibits government access to personal data in educational records without a court order or lawfully issued subpoena, unless the government is seeking access to the records for a specified education-related purpose. Vests administrative enforcement of the Act in the Department of Education, and provides for termination of Federal funds if an institution violates the Act and compliance cannot be secured voluntarily.

Freedom of Information Act (5 U.S.C. § 552) - Provides individuals with access to many types of records that are exempt from access under the Privacy Act, including many categories of personal information. Unlike those of the Privacy Act, FOIA procedures are available to non-resident foreign nationals. 5 U.S.C. § 552.

Health Research Data Statute (42 U.S.C. § 242m) - Prohibits disclosure of data collected by the National Centers for Health

Services Research and for Health Statistics in any way that would identify an individual.

Mail Privacy Statute (39 U.S.C. § 3623) - Prohibits the opening of mail without a search warrant or the addressee's consent.

Paperwork Reduction Act of 1980 (44 U.S.C. § 3501, et seq.) - Prohibits an agency from collecting information from the public if another agency has already collected the same information, or if the Office of Management and Budget does not believe the agency either needs or can make use of the information. Requires each Federal data collection form to explain why the information is being collected, how it is to be used, and whether the individual's response is mandatory, required to obtain a benefit, or voluntary.

Privacy Act (5 U.S.C. § 552a) - Mandates that personal data be collected as much as possible directly from the record subject. Generally prohibits collection of information about an individual's exercise of First Amendment rights (e.g., freedom of expression, assembly, and religion). Requires that when an agency requests information about an individual, it notify the individual of the agency's authorization and purpose for collecting information, the extra-agency disclosures ("routine uses") that may be made of the data collected, and the consequences to the individual for failing to provide the information. Requires agencies, on request, to provide individuals with access to records pertaining to them and an opportunity to correct or challenge the contents of the records.

Restricts Federal agencies from disclosing personal data except for publicly announced purposes, and requires agencies (1) to keep an accounting of extra-agency disclosures, (2) to instruct record management personnel in the requirements of the Act and the rules for its implementation, and (3) to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records."

Places accountability for the handling of personal records on the recordkeeping agency and its employees. Requires agencies to publish a detailed annual notice that describes each record system, the kind of information maintained, its sources, the policies governing management of the system, and the procedures for individuals to obtain access to records about themselves.

Allows an individual harmed by a violation of the Act to sue the agency for an injunction, damages, and court costs. It also provides criminal penalties -- fines of up to $5,000 -- against employees who disclose records in violation of the Act.

Privacy Protection Act (42 U.S.C. § 2000aa) - Prohibits government agents from conducting unannounced searches of press offices and files if no one in the press office is suspected of a crime. Requires instead that the government request voluntary cooperation or subpoena the material sought, giving the holder of the material a chance to contest the action in court. Directs the U.S. Attorney General to issue guidelines for seeking evidence from other non-suspect third parties, with special consideration to such traditionally confidential relationships as doctor-patient and priest-penitent.

Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.) - Requires Federal agencies seeking access to private financial records either (1) to notify the subject of the purpose for which the records are sought and provide the subject with an opportunity to challenge the disclosure in court, or (2) to obtain a court order for direct access to the records if notice would allow the record subject to flee or destroy the evidence. Prohibits a Federal agency that has obtained access to an individual's financial records from disclosing the records to another agency without (1) notifying the individual and (2) obtaining certification from the receiving agency that the records are relevant to a legitimate law enforcement inquiry of the receiving agency. Where a government agency or a financial institution discloses records or information in violation of the Right to Financial Privacy Act, the agency or institution is liable to the customer for any actual damages sustained, a $100 penalty, punitive damages for willful or intentional violations, court costs, and attorney's fees.

Tax Reform Act (26 U.S.C. §§ 6103, 6108, 7609) - Requires notice and opportunity-to-challenge procedures (similar to those of the Right to Financial Privacy Act) before the Internal Revenue Service may obtain access to certain institutional records about an individual in the hands of certain private recordkeepers. Strictly limits disclosure of tax returns and return information, and in some cases requires a court order for disclosures to law enforcement agencies for purposes unrelated to tax administration.

Video Privacy Protection Act (18 U.S.C. § 2710) - Affords users and purchasers of commercial videotapes rights similar to those of patrons of libraries. Prohibits videotape sale or rental companies from disclosing customer names and addresses, and the subject matter of their purchases or rentals for direct marketing use, unless the customers have been notified of their right to prohibit such disclosures. Restricts videotape companies from disclosing personal data about customers without customers' consent or court approval. Requires that subscribers be notified and provided with an opportunity to contest a data request prior to a judicial determination. Video companies that violate the Video Privacy Protection Act may be liable for damage awards of at least $2500, punitive damages, costs, and attorneys fees.

Wiretap Statutes (18 U.S.C. § 2510, et seq.; 47 U.S.C. § 605) - Prohibits the use of eavesdropping technology and the interception of electronic mail, radio communications, data transmission and telephone calls without consent. 18 U.S.C. § 2510, et seq.; 47 U.S.C. § 605. The Federal Communications Commission also has a rule and tariff prescription prohibiting the recording of telephone conversations without notice or consent. See 47 C.F.R. §64.501; 5 FCC Red 502 (1987).

STATE CONSTITUTIONS

Many State constitutions restrict intrusive collection practices by State governments. See, e.g., Alaska Const. Art. 1, § 22; Ariz. Const. Art. II, § 8; Calif. Const. Art. I, § 1; Fla. Const. Art. 1, § 23; Haw. Const. Art. 1, § 5; Ill. Const. Art. 1, § 6; La. Const. Art. 1, § 5; Mont. Const. Art II, § 10; N.Y. Const. Art. 1, § 12; Pa. Const. Art. 1, § 1; S.C. Const. Art. 1, § 10; Wash. Const. Art. 1, § 7.

STATE LAWS

Bank Records Statutes - Prohibit financial institutions from disclosing financial records of a customer to a third party without either the customer's consent or legal process. See, e.g., Ill. Rev. Stat. ch. 16 1/2, § 148.1; Me. Rev. Stat. § 16; Md. Fin. Inst. Code §1-302. Mass. Gen. Laws ch. 167B, §16; Okla. Stat. tit. 6, § 2201-2206; Or. Rev. Stat. § 192.550.

Cable Television Statutes - Permit subscribers to correct information or have their names deleted from data files maintained by cable operators. Prohibit disclosure of personal information collected by a cable operator unless the subscriber has had notice and has not objected to the disclosure. See, e.g., Cal. Penal Code § 637.5; Conn. Gen. Stat. § 53422; Ill. Stat. ch. 38, § 87-2; Wis. Stat. § 134.43.

Common Law Remedies - Provide redress for invasion of privacy (i.e., intrusions into places or affairs as to which an individual has a reasonable expectation of privacy), public disclosure of private facts, defamation (i.e., disclosures of inaccurate personal information), and breach of duty of confidentiality. Provide for money damages and, in some cases, nominal, special or punitive damages, and injunctive relief. See generally, W. Prosser, The Law of Torts (5th ed. 1984).

Computer Crime Statutes - Prohibit individuals from tampering with computers or accessing certain computerized records without authorization. Persons engaged in such conduct are subject to criminal penalties, civil damages, or both. See, e.g., Ala. Code § 13A-8-101; Alaska Stat. §§ 11.81.900(b)(44),

11.46.200(a); Ariz. Rev. Stat. §§ 13-2301E, 13-2316; Cal. Penal Code §§ 502, 631, 632, 637.2; Colo. Rev. Stat. § 18-5.5-101; Conn. Gen. Stat. § 53a-250; Del. Code tit. 11, §§ 931 to 939; Fla. Stat. §§ 815.01, 934.21, et seq.; Ga. Code § 16-9-90; Haw. Rev. Stat. §§ 708-890, 803-47.5; Idaho Code § 18-22; Ill. Rev. Stat. ch. 38, § 16-9; Ind. Code § 35-43-1-4; Iowa Code § 716A; Kan. Stat. § 21-3755; Ky. Rev. Stat. § 434; La. Rev. Stat. § 14:73.1; Mass. Gen. Laws ch. 266, § 30(2); Md. Cts. & Jud. Proc. Code §§ 10-402, 10-410, 10-4A-01, 10-4A-08; Mich. Comp. Laws ch. 266, § 752.791; Minn. Stat. §§ 609.87, 626A.26, et seq.; Miss. Code § 97-45-1; Mo. Stat. § 569.093; Mont. Code § 45-6-310; Neb. Rev. Stat. §§ 28-1343, 86-707.09; Nev. Rev. Stat. § 205.473; N.H. Rev. Stat. § 638:16; N.J. Rev. Stat. §§ 2A:38A-1, 2C:20-1; N.M. Stat. § 30-16A-1; N.Y. Penal Law § 156; N.C. Gen. Stat. § 14-453; N.D. Cent. Code § 12.1-06.1-08; Ohio Rev. Code §§ 2901.01, 2913.01; Okla. Stat. tit. 21, §§ 1951 to 1956; Or. Rev. Stat. §164.377; Pa. Stat. tit. 18, §§ 3933, 5471, et seq.; R.I. Gen. Laws § 11-52-1; S.C. Code § 16-16-10; S.D. Codified Laws § 43-43B-7; Tenn. Code § 39-3-14-4; Tex. Penal Code §§ 16.04, 33.01; Tex. Crim. Proc. Code Art. 18.21; Utah Code §§ 76-6-701, 77-23b, et seq.; Va. Code § 18.2-152.1; Wash. Rev. Code § 9A.48.100; Wis. Stat. § 943.70; Wyo. Stat. § 6-3-501.

Credit Reporting Statutes - Prohibit collection by creditors of information on race, religion, or sex. Restrict disclosure by credit reporting agencies of credit information to third parties. See, e.g., Cal. Civil Code § 1786; Kan. Stat. § 50-703; Ky. Rev. Stat. § 344.370; Me. Rev. Stat. § 1311; Md. Comm. Law Codes § 14-1201; N.H. Rev. Stat. § 359-B; N.Y. Gen. Bus. Law § 380; Wash. Rev. Code § 49.60.175.

Criminal Justice Information Statutes - Require law enforcement agencies to permit individuals to see, copy, and correct information about themselves maintained in the criminal justice information systems. Require that criminal justice information be reported promptly, completely, and in standard format. These statutes also have quality control requirements for computerized information systems and special requirements that arrest records indicate the disposition of the case. In addition, most of the State criminal justice information statutes require strict security measures to protect this information. See, e.g., Ala. Code § 41-9-643; Alaska Stat. §§ 12.62.010, 12.62.040; Cal. Penal Code §§ 11075-81, 11121-26; Colo. Rev. Stat. § 24-72-308; Del. Code tit. 11, § 8511; D.C. Code § 4-131; Fla. Stat. § 943.056; Ga. Code § 35-3-37; Haw. Rev. Stat. §§ 846.1, 831-3.2; Idaho Code § 4812(2)(o); Ill. Stat. ch. 38, § 206-5; Iowa Code §§ 692.5, 749B.12; Ky. Rev. Stat. § 61.884; Me. Rev. Stat. tit. 16, § 620; Md. Code art. 27, § 742; Mass. Gen. L. ch. 6, §§ 167-178; Mont. Code § 44-5-101; N.D. Cent. Code § 12-60-16; Neb. Rev. Stat. 29-3523; Nev. Rev. Stat. §§ 179.245, 179.255; N.J. Rev. Stat. § 2A:164-28; S.C. Code § 73-22; Va. Code §§ 9-192, 19.2-389.

Employment Records Statutes - Prohibit employers from collecting information about a job applicant's race, sex, color, religion, national origin, and other attributes. Allow individuals access to personnel records held by their employers. See, Cal. Lab. Code § 1198.5; Colo. Rev. Stat. § 24-24-301; Conn. Gen. Stat. § 31-128a; Del. Code tit. 19, § 723; Hawaii Rev. Stat. § 378-1; Ill. Stat. ch. 48, § 2001; Me. Rev. Stat. tit. 26, § 631; Mass. Gen. Laws ch. 149, § 52C; Mich. Comp. Laws § 423.501; Nev. Rev. Stat. § 613.075; N.H. Rev. Stat. § 275.56; Ohio Rev. Code § 4113.23; Or. Rev. Stat. § 652.750; Pa. Stat. tit. 43, § 1321; R.I. Gen. Laws § 28-6.4-1; S.D. Codified Laws § 3-6A-31; Wash. Rev. Code 49.12.250.

Fair Information Practices Statutes - Limit the type of information that State governments can collect and maintain about individuals. Allow individuals to inspect and challenge information about them held by the State. Restrict the ability of State governments to disclose personal data to third parties. See Ala. Code § 41-8-10; Alaska Stat. § 09.25.140; Ark. Stat. § 16-804; Cal. Civil Code § 1798; Colo. Rev. Stat. §§ 24-72.204(3)(a), 24-90-119; Conn. Gen. Stat. § 4-190; D.C. Code § 37-106.2; Fla. Stat. § 257.261; Ill. Stat. ch. 116, § 43.5; Ill. Stat. ch. 81, § 1202; Ind. Code §§ 4-1-6, 5-14-3-1; Iowa Code § 68A.7(13); Ky. Rev. Stat. §§ 61.870, 61.884; La. Rev. Stat. § 44:13; Mass. Gen. L. ch. 119, § 51E; Mass. Gen. L. ch. 66, § 17A; Me. Rev. Stat. tit. 27, § 121; Me. Rev. Stat. tit. 5, § 1851; Mich. Comp. Laws § 397.603; Minn. Stat. § 13.01; Miss. Code §25-53-53; Mo. Stat. § 182.817; Mont. Rev. Code § 22-1-1103; Neb. Rev. Stat. § 84-712.05; Nev. Rev. Stat. § 239.013; N.J. Rev. Stat. § 18A:73-43.2; N.Y. Civ. Prac. L. & R. § 4509; N.Y. Pub. Off. Law § 91; N.C. Gen. Stat. § 125-19; N.D. Cent. Code 40-38-12; Ohio Rev. Code § 1347.01; Okla. Stat. tit. 74, § 118.17; Or. Rev. Stat. § 192.500(i)(j); Pa. Stat. tit. 24, § 4428; R.I. Gen. Laws § 38-2-2(21; S.C. Code § 60-4-10; S.D. Codified Laws § 14-2-51; Utah Code § 63-50-10; Va. Code §§ 2.1-342, 2.1-377; Wash. Rev. Code § 43.105.040(4); Wis. Stat. § 43:30; Wyo. Stat. § 16-4-203(d).

Insurance Records Statutes - Require insurers to provide general information about their personal data practices to applicants and policyholders, with further information available upon request. Also require them to notify applicants about the collection and disclosure of personal data, and to specify when information is requested solely for marketing or research purposes. Restrict the use of "pretext interviews" (in which the identity or purpose of the interviewer is misrepresented) and require specific consent forms to be used for the collection of information that requires authorization from an individual. Permit individuals who are denied insurance to learn the specific reasons for such denial and to obtain access to the information used in refusing coverage.

Applicants or policyholders also may obtain access to non-privileged personal information about them, and may propose that such information be corrected, amended, or deleted. Except where such disclosure is permitted by law, these statutes prohibit insurers from disclosing without the individual's consent information they collect on individuals. See, e.g., Calif. Ins. Code § 791, Ill. Stat. ch. 73, §§ 1001-1024.

Media Shield Statutes - Permit journalists to refuse to identify the sources of information received in the course of professional employment. See, e.g., Ariz. Rev. Stat. nn. § 12.2237; R.I. Gen. Laws § 9-19.1-1.

Medical Records Statutes - Allow individuals to have access to their medical records. Limit the use and disclosure of medical or mental health records. See, e.g., Alaska Stat. § 47.30.260; Cal. Civil Code § 56; Cal. Health & Safety Code § 25250; Colo. Rev. Stat. § 25-1-801, 18-4-412; Conn. Gen. Stat. § 4-105, 51-146h; Fla. Stat. §§ 455.241, 395.017; Ill. Stat. ch. 91 1/2. § 801; Ind. Stat. § 34-3-15.5-4; La. Rev. Stat. § 40:2014.1; Mass. Gen. Laws ch. 111 § 70E; Minn. Stat. § 144.335; Nev. Rev. Stat. §§ 629.061, 49.215-245; N.M. Stat. § 42-1-15; Okla. Stat. tit. 76, § 19; Pa. Stat. tit. 50, § 7111; R.I. Gen. Laws § 5-37.3.3; Tenn. Code § 53-1322, 10-7-504; Tex. Rev. Civ. Stat. art. 4447d; Va. Code § 8.01-413; Wisc. Stat. § 146.83.

Polygraph Test Statutes - Restrict the use of mandatory polygraph tests as a condition for employment. See, e.g., Alaska Stat. § 23.10.37; Ala. Code § 34-25-32; Ariz. Rev. Stat. § 32-2701; Ark. Stat. § 17-32-211; Cal. Gov't. Code § 3307; Cal. Labor Code § 432.2; Conn. Gen. Stat. § 31-51g; Del. Code tit. 19, § 704; D.C. Code §§ 36-801 to 36-803; Haw. Rev. Stat. § 378.21; Idaho Code §44-903; Iowa Code § 730.4; La. Stat. § 37:2848; Me. Rev. Stat. tit. 32, § 7166; Md. Code art. 100, § 95; Mass. Gen. Laws ch. 149, § 19B; Mich. Comp. Laws § 37.201; Minn. Stat. § 181.75; Miss. Code § 73-29-31; Mont. Rev. Codes § 39.2-304; Nev. Rev. Stat. § 648; N.J. Stat. § 2C:40A-1; N.M. Stat. § 61-26-9; N.Y. Labor Law § 733; Okla. Stat. § 1468; Or. Rev. Stat. § 659.225; Pa. Cons. Stat. § 7321; R.I. Gen. Laws § 28-6.1.1; S.C. Code § 40-53-80; Tenn. Code § 62-27-123; Tex. Rev. Civ. Stat. art. 4413(29cc); Utah Code § 34-37-16; Ver. Stat. § 5a; W.Va. Code § 21-5-5a; Wis. Stat. § 111.37.

Privilege Statutes - Limit the introduction into legal proceedings of personal information maintained by professionals such as doctors, psychotherapists, attorneys, clergy, and accountants concerning individuals with whom they have a professional relationship. See Ala. Code tit. 34-26.2; Alaska Stat. §§ 47.30.260, 08.86.200; Ariz. Rev. Stat. § 12-2235; Ark.

Stat. §§ 28-607, 72-1616; Cal. Evid. Code § 1010; Colo. Rev. Stat. § 3-90-107; Conn. Gen. Stat. § 52-146; Del. Code tit. § 3518; D.C. Code § 14-307; Fla. Stat. § 90.542; Ga. Code §§ 24-9-21, 43-3-32; Haw. Rev. Stat. § 621.20; Idaho Code §§ 9-203(4), 54-2314; Ill. Stat. ch. 51 §§ 5.1, 5.2; Ind. Code § 34-1-14-5; Iowa Code § 622.10; Ky. Rev. Stat. §§319.111, 421.210, 231.200, 421.215; La. Rev. Stat. §§ 15:476, 37:2366, 13:3734; Me. Rev. Stat. tit. 32, § 3153; Md. Code art. 35, § 13A; Md. Courts Code §§ 9-100, 9-108, 9-109, 9-111; Mich. Comp. Laws §§ 338-1018, 600.2156, 600.2157; Minn. Stat. § 595.02; Miss. Code §§ 13-1-21, 73-31-29; Mo. Stat. § 491.060; Mont. Rev. Codes §§ 93-701-4, 66-3212; Neb. Rev. Stat. §§ 27-503 to 27-508; Nev. Rev. Stat. §§ 49.125, 49.215, 49.255; N.H. Rev. Stat. §§ 329:26, 330-A:19; N.J. Rev. Stat. §§ 2A:34A-23, 2A:84A-22.2-9, 45:8B-29; N.Y. Civ. Prac. L. & R. §§ 4504, 4505, 4507, 4508; N.C. Gen. Stat. §§ 8-53.2, 130-184, 130-95; Ohio Rev. Code §§ 4732.9, 2317.02; Okla. Stat. tit. 12, § 385; Okla. Stat. tit. 59, § 1372; Or. Rev. Stat. § 44.040; R.I. Gen. Laws § 9-17-23; S.D. Codified Laws §§ 19-2-3, 19-2-2; Tenn. Code §§ 24-1-206, 24-1-207, 62-143; Tex. Rev. Civ. Stat. art. 3715a; Tex. Rev. Civ. Stat. art. 5561h, § 13(d); Utah Code §§ 58-25-9, 58-35-10, 58-39-10, 78-24-8; Va. Code § 8.01-399; Wash. Rev. Code §§ 18.83.110, 18.53.200, 5.60.050, 5.60.060, 10.52.020; Wis. Stat. §§ 455.09, 885.20, 885.21; Wyo. Stat. §§ 1-139, 33-343.4.

School Records Statutes - Permit students and their parents to inspect and challenge the accuracy and completeness of school records. Limit the ability of schools to disclose information from school records to third parties. See, e.g., Ariz. Rev. Stat. § 15-151; Cal. Educ. Code §49060; Conn. Gen. Stat. §§ 10-154a, 10-15b; Del. Code tit. 14, § 4111; Fla. Stat. 232.23; Idaho Code § 9-203(6); Ill. Rev. Stat. ch. 122, § 50-1; Iowa Code 22.7; Ky. Rev. Stat. § 421.216; Mass. Gen. Laws ch. 71, §§ 34A, 34E; Me. Rev. Stat. tit. 20A, § 6001; Mich. Comp. Laws § 600.2165; Miss. Code § 37-15-3; Mont. Rev. Codes § 93-701-4; N.C. Gen. Stat. § 8-53-4; N.D. Cent. Code § 31-06.1; Neb. Rev. Stat. § 79-4.157; Ohio Rev. Code 3319.321; Okla. Stat. tit. 70, § 6-115; Or. Rev. Stat. § 336.195; S.D. Codified Laws § 19-2-5.1; Tenn. Code § 10-7-504; Tex. Rev. Civ. Stat. art. 6252-17a, § 3(a)(14); Vt. Stat. tit. 1, § 317(11); Va. Code § 2.1-342(b)(3); Wash. Rev. Code § 42-17.310; Wis. Stat. § 118.125; Wyo. Stat. § 9-692.3(3)(d).

Stored Wire Communications Statutes - Require notice to subscribers before the government can access stored wire communications. See, e.g., Ariz. Rev. Stat. § 13-3016; Fla. Stat. § 934.23; Haw. Rev. Stat. § 803-47.6; Md. Cts. & Jud. Proc. § 10-4A-04; Minn. Stat. § 626A.28; Pa. Cons. Stat. § 5743; Tex. Crim. Proc. Code Art. 18.21; Utah Code § 77-23b-4; Va. Code § 19.2-70.3.

Tax Return Statutes - Prohibit disclosure by the government of State tax returns and return information. See Alaska Stat. § 9.25.100; Ariz. Rev. Stat. § 43.145; Colo. Rev. Stat. § 39-21-113; Del. Code tit. 30, § 1241; Ga. Code § 48-7-60; Haw. Rev. Stat. § 235.116; Idaho Code § 63-3077; Kan. Stat. § 131.190; Ky. Rev. Stat. § 131.190; La. Rev. Stat. § 47:1508; Me. Rev. Stat. tit. 36, § 5340; Md. Tax Gen. Code §13-202; § 300; Mass. Gen. Laws ch. 62C, §74; Minn. Stat. § 290-611; Neb. Rev. Stat. § 77-27; N.Y. Tax Law § 697; N.C. Gen. Stat. § 105-259; N.D. Cent. Code § 57-38-57; Ohio Rev. Code § 5747.18; Okla. Stat. tit. 68, § 205; Or. Rev. Stat. § 314.835; R.I. Gen. Laws § 44-30-95(c); S.C. Code § 12-35-1530; Tenn. Code § 67-131; Utah Code § 59-1-403; Va. Code § 2.1-342(b); Wash. Rev. Code § 42.17.310; W. Va. Code § 11-21-80; Wis. Stat. § 71.78.

Uniform Commercial Code - Encourages financial institutions to disclose to their customers in a timely fashion the record of all transactions by holding the financial institution responsible for any errors until after the customer is informed of the bank's version of what has occurred. See e.g., Tenn. Code § 47-4-406.

Video Privacy Statutes - Restrict videotape sales or rental companies from disclosing personal data about customers without their consent. See, e.g., Cal. Civil Code § 1799.3; Del. Code tit. 11, § 925.

Wiretap Statutes - Restrict electronic eavesdropping and interception of communications by wire or radio. See Ala. Code tit. 13A, § 11.30; Alaska Stat. § 11.60.290; Ariz. Rev. Stat. § 13:1051; Ark. Stat. § 73-1810; Cal. Penal Code §§ 631 to 637; Colo. Rev. Stat. §§ 18-9-301, 16-15-101; Conn. Gen. Stat. 54-41a; Del. Code tit. 11, § 1335; D.C. Code § 23:541; Fla. Stat. § 934.01; Ga. Code §16-11-62; Haw. Rev. Stat. § 711-1111; Idaho Code § 18-6701; Ill. Rev. Stat. ch. 134, § 15a; Iowa Code § 716.7-8; Kan. Stat. § 22-2514; Ky. Rev. Stat. § 526.010; La. Rev. Stat. § 14:322; Me. Rev. Stat. tit. 15, § 709; Md. Cts. & Jud. Proc. Code § 10-401; Mass. Gen. Laws ch. 272, § 99; Mich. Comp. Laws § 750-539; Minn. Stat. § 626A.01; Neb. Rev. Stat. § 86-701; Nev. Rev. Stat. § 200.610; N.H. Rev. Stat. § 570-A:1; N.J. Rev. Stat. § 2A:156A-1; N.M. Stat. § 30-12-2; N.Y. Crim. Proc. Law § 700.05; N.C. Gen. Stat. § 14-155; N.D. Cent. Code § 12.1-15-02; Ohio Rev. Code § 2933.58; Pa. Cons. Stat. § 5703; R.I. Gen. Laws § 12-35-21; S.D. Codified Laws § 23-13A-1; Tenn. Code 39-3-1324; Tex. Rev. Stat. Penal Code 16.02; Utah Code § 77-54(A)-1; Va. Code § 19.2-61; Wash. Rev. Code § 9.73.030; W. Va. Code § 61-3-246; Wis. Stat. § 968.27. Some states also have tariff prescriptions requiring common carriers operating within their jurisdictions to terminate subscribers who record telephone conversations without notice or consent.

APPENDIX 2

PARTIAL LIST OF UNITED STATES PRIVACY LAWS

This list provides examples of United States privacy laws that, taken together, ensure an adequate level of protection for personal data. It includes Federal constitutional and statutory law, and State constitutional, statutory, and common law. Laws affecting government information practices are discussed separately from those affecting private sector record keepers.

The laws for each sector are listed under four categories: (1) rights of data subjects (e.g., right to notification, access, or participation); (2) obligations of processors of personal data (e.g., limits on collection, use, or disclosure); (3) data quality and security; and (4) accountability, sanctions, and remedies. These categories identify the principles underlying the personal data directive of the Council of the European Communities.

Because many of the cited laws provide a variety of protections for a single type of record, many are cited under more than one category. The list is divided into parts as follows:

A. Government: Rights of Data Subjects
B. Government: Obligations of Processors of Personal Data
C. Government: Data Quality and Security
D. Government: Accountability, Sanctions, and Remedies
E. Private Sector: Rights of Data Subjects
F. Private Sector: Obligations of Processors of Personal Data
G. Private Sector: Data Quality and Security
H. Private Sector: Accountability, Sanctions, and Remedies

Federal statutes and regulations are cited by reference to the United States Code (U.S.C.) and the Code of Federal Regulations (C.F.R.). Constitutional provisions are cited by the leading judicial decisions interpreting them. State law generally is cited by reference to State codes. In some instances, State law is cited by example --- statutes or judicial decisions in a particular State which illustrate a proposition about the law of many or most States. Occasionally a well-known treatise such as Prosser's Law of Torts is cited in support of a particular common law rule.

Also cited are two model laws: (1) the National Association of Insurance Commissioners' Insurance Information and Privacy Protection Model Act (NAIC Model Law); and (2) the Uniform Information Practices Code, drafted in 1980 by the

National Conference of Commissioners on Uniform State Laws to provide a guide for State legislation similar to the Federal Privacy and Freedom of Information Acts. Although model laws have no legal force, they usually have a significant influence on further legislation in the area. Since the issuance of the NAIC Model Law, 13 States have enacted it or similar legislation. See, Ariz. Rev. Stat. §§ 20-21-1 to 20-2120; Cal. Ins. Code §§ 791.01 to 791.26; Conn. Gen. Stat. §§ 38-501 to 38-523; Ga. Code §§ 33-39-1 to 33-39-23; Ill. Rev. Stat. ch. I.C. §§ 1001 to 1024; Kan. Stat. §§ 2.111 to 2.113; Minn. Stat. §§ 72A.49 to 72A.505; Mont. Code §§ 33-19-101 to 33-19-409; Nev. Admin. Code §§ 679B.560 to 679B.750; N.J. Rev. Stat. §§ 17:23A-1 to 17:23A-22; N.C. Gen. Stat. §§ 58-39-1 to 58-39-120.; Or. Rev. Stat. §§ 746.600 to 746.690; and Va. Code §§ 38.2-600 to 38.2-620.

For further information about U.S. privacy statutes, a useful reference work is Robert Ellis Smith's Compilation of State and Federal Privacy Laws (1988 ed.), published by Privacy Journal, P.O. Box 8844, Washington, D.C. 20003.

This list was prepared by the law firm of Piper & Marbury.

A. Government: Rights of Data Subjects

1. The Fifth and Fourteenth Amendments to the Constitution prohibit Federal and State and local governments from depriving a person of "life, liberty, or property" without "due process of law." The procedures required by the courts in applying this principle are designed to assure that the individual has a reasonable opportunity to challenge the proposed deprivation. At a minimum, there must be notice and a hearing at which the factual basis of the decision is subject to scrutiny. See Mullane v. Central Hanover Bank & Trust Co., 337 U.S. 306, 314 (1950); Greene v. McElroy, 360 U.S. 474, 496-497 (1959); Goldberg v. Kelly, 397 U.S. 254, 269-271 (1970).

2. The Administrative Procedure Act sets out detailed procedures for Federal agencies' conduct of administrative hearings required by the Constitution or by statute. The Act's provisions prescribe, for example, how notice is to be given and how evidence may be collected, presented, and evaluated. 5 U.S.C. §§ 551, 554-558.

3. The Privacy Act requires agencies, on request, to provide individuals with access to records pertaining to them and an opportunity to correct or challenge the contents of the records. 5 U.S.C. § 552a.

4. The Freedom of Information Act provides individuals with access to many types of records that are exempt from access under the Privacy Act, including many categories of personal information. 5 U.S.C. § 552.

5. Most of the State fair information practice statutes allow individuals to inspect and challenge information about them held by the State; many also require some type of registry or inventory of State-maintained data bases. See, e.g., Va. Code § 2.1-377; Mass. Gen. Laws ch. 66A; Ark. Stat. § 16-804; Cal. Civ. Code § 1798; Colo. Rev. Stat. §§ 24-72-204(3)(a), 24-90-119; Conn. Gen. Stat. § 4-190; Ill. Stat. ch. 116 § 43.5; Ind. Code §§ 5-14-3-1, 4-1-6-3; Ky. Rev. Stat. § 61.884; Mo. Stat. § 182.817; Nev. Rev. Stat. § 229.013; N.Y. Pub. Off. Law § 91; Ohio Rev. Code § 1347.01; Utah Code § 63-50-1.

6. Except in cases of judicially-sanctioned search warrants, the Electronic Communications Privacy Act of 1988 requires that subscribers be notified and provided with an opportunity to contest in court a government entity's request for access to electronic mail or other stored communications in the control of a provider of electronic communications services or remote computing services. 18 U.S.C. §§ 2703, 2704.

Several States have enacted similar stored communications statutes entitling subscribers to notice prior to governmental access to such communications. See, e.g., Ariz. Rev. Stat. § 13-3016; Fla. Stat. § 934.23; Haw. Rev. Stat. § 803-47.6; Md. Cts. & Jud. Proc. § 10-4A-04; Minn. Stat. § 626A.28; Pa. Cons. Stat. § 5743; Tex. Crim. Proc. Code Art. 18.21; Utah Code § 77-23b-4; Va. Code § 19.2-70.3.

7. The Video Privacy Protection Act of 1988 requires, except in cases of judicially-sanctioned search warrants, that customers be notified and provided with an opportunity to contest a government entity's request for access to a videotape sale or rental company's records containing personal data about the customer. 18 U.S.C. § 2710.

8. The Right to Financial Privacy Act requires Federal agencies seeking access to private financial records either (1) to notify the subject of the purpose for which the records are sought and provide an opportunity to challenge the disclosure in court, or (2) to obtain a court order for direct access to the records if notice would allow the record subject to flee or destroy the evidence. 12 U.S.C. § 3401, et seq.

Moreover, a Federal agency that has obtained access to an individual's financial records is prohibited from disclosing the records to another agency without notifying the individual and obtaining certification from the receiving agency that the records are relevant to a legitimate law enforcement inquiry of the receiving agency. Id.

9. Some states prohibit financial institutions from disclosing financial records of a customer to the government without either the customer's consent or legal process. See, e.g., Ill. Rev. Stat. ch. 16-1/2, § 148.1; Me. Rev. Stat.

§ 161; Md. Code art. 11, § 225; Okla. Stat. tit. 6, §§ 2201-2206.

10. Under the Cable Communications Policy Act of 1984, subscribers must be notified of any effort by a government entity to obtain judicial approval for access to personal data collected by a cable television company about its subscribers, and be provided with an opportunity to contest a government's claims that the data is likely to reveal criminal activity. 47 U.S.C. § 551(h). Some States also have enacted statutes which enable cable subscribers to restrict the government's ability to obtain access to personal data on the subscriber collected by cable companies. See, e.g., Cal. Penal Code § 637.5; Ill. Stat. ch. 38, § 87-2; Conn. Gen. Stat. § 53-421; Wis. Stat. § 134.43.

11. Under the Family Educational Rights and Privacy Act, students and their parents may inspect and challenge the accuracy and completeness of education records maintained about the students. Additionally, the Act requires that students and their parents be informed of their statutory rights under the Act. 20 U.S.C. § 1232g.

12. A number of State statutes permit students and their parents to inspect and challenge the accuracy and completeness of school records. See, e.g., Ariz. Rev. Stat. § 15-151; Cal. Educ. Code § 49060; Conn. Gen. Stat. § 10-15b; Del. Code tit. 14, § 4111; Fla. Stat. 232.23; Ill. Rev. Stat. ch. 122, § 50-1; Mass. Gen. Laws ch. 71, §§ 34A, 34E; Neb. Rev. Stat. § 79-4.157; Or. Rev. Stat. § 336.195; Tex. Rev. Civ. Stat. art. 6252-17a, § 3(a)(14); Va. Code §2.1-342(b)(3); Wash. Rev. Code § 42.17.310; Wyo. Stat. § 9-692.3(d).

13. Consent is required in most states for introducing into legal proceedings, personal information maintained by professionals such as doctors, psychotherapists, attorneys, clergy, and accountants on individuals with whom they have a relationship. See Ala. Code tit. 34-26.2; Alaska Stat. §§ 47.30.260, 08.86.200; Ariz. Rev. Stat. § 12-2235; Ark. Stat. §§ 28-607, 72-1616; Cal. Evid. Code § 1010; Colo. Rev. Stat. § 3-90-107; Conn. Gen. Stat. § 52-146; Del. Code tit. § 3518; D.C. Code § 14-307; Fla. Stat. § 90.542; Ga. Code §§ 24-9-21, 43-3-32; Haw. Rev. Stat. § 621.20; Idaho Code §§ 9-203(4), 54-2314; Ill. Stat. ch. 51 §§ 5.1, 5.2; Ind. Code § 34-1-14-5; Iowa Code § 622.10; Ky. Rev. Stat. §§319.111, 421.210, 231.200, 421.215; La. Rev. Stat. §§ 15:476, 37:2366, 13:3734; Me. Rev. Stat. tit. 32, § 3153; Md. Code art. 35, § 13A; Md. Courts Code §§ 9-100, 9-108, 9-109, 9-111; Mich Comp. Laws §§ 338-1018, 600.2156, 600.2157; Minn. Stat. § 595.02; Miss. Code §§ 13-1-21, 73-31-29; Mo. Stat. § 491.060; Mont. Rev. Codes §§ 93-701-4, 66-3212; Neb. Rev. Stat. §§ 27-503 to 27-508; Nev. Rev. Stat. §§ 49.125, 49.215, 49.255; N.H. Rev. Stat. §§ 329:26, 330-A:19; N.J. Rev. Stat. §§ 2A:34A-23,

2A:84A-22.2-9, 45:8B-29; N.Y. Civ. Prac. L. & R. §§ 4504, 4505, 4507, 4508; N.C. Gen. Stat. §§ 8-53.2, 130-184, 130-95; Ohio Rev. Code §§ 4732.9, 2317.02; Okla. Stat. tit. 12, § 385; Okla. Stat. tit. 59, § 1372; Or. Rev. Stat. § 44.040; R.I. Gen. Laws § 9-17-23; S.D. Codified Laws §§ 19-2-3, 19-2-2; Tenn. Code §§ 24-1-206, 24-1-207, 62-143; Tex. Rev. Civ. Stat. art. 3715a; Tex. Rev. Civ. Stat. art. 5561h, § 13(d); Utah Code §§ 58-25-9, 58-35-10, 58-39-10, 78-24-8; Va. Code § 8.01-399; Wash. Rev. Code §§ 18.83.110, 18.53.200, 5.60.050, 5.60.060, 10.52.020; Wis. Stat. §§ 455.09, 885.20, 885.21; Wyo. Stat. §§ 1-139, 33-343.4.

14. A number of states also have enacted statutes which require the subject's consent prior to use of polygraph tests by government agencies. See, e.g., Ala. Code § 34-25-32; Ariz. Rev. Stat. § 32-2701; Ark. Stat. § 17-32-211; Cal. Gov't. Code § 3307; La. Stat. § 37:2848; Md. Code art. 100, §95; Miss. Code § 73-29-31; Nev. Rev. Stat. § 648; N.M. Stat. § 61-26-9; Okla. Stat. § 1468; S.C. Code § 40-53-80; Tenn. Code § 62-27-123; Tex. Rev. Civ. Stat. § 4413(29cc); Wis. Stat. § 111.37.

15. Federal law requires that Federally-funded State and local criminal justice information systems include information on the disposition of any arrest, and provide for individuals to be able to see, copy, and correct information about themselves in the system. 42 U.S.C. § 3789g.

16. Many State laws require law enforcement agencies to permit individuals to see, copy, and correct information about themselves maintained in the Criminal Justice Information Systems. See, e.g., Ala. Code § 41-9-643; Alaska Stat. § 12.62.010; Cal. Penal Code §§ 11075-81, 11121-26; Colo. Rev. Stat. § 24-72-308; Del. Code tit. 11, § 8511; D.C. Code § 4-131; Fla. Stat. § 943.056; Ga. Code § 35-3-37; Haw. Rev. Stat §§ 846.1, 831-3.2; Idaho Code § 4812(2)(o); Ill. Stat. ch. 38, § 206-5; Iowa Code § 692.5; Ky. Rev. Stat. § 61.884; Me. Rev. Stat. tit. 16, § 620; Md. Code art. 27, § 742; Mass. Gen. L. ch. 6, §§ 167-178; Mont. Code § 44-5-101; Neb. Rev. Stat. 29-3523; Nev. Rev. Stat. §§ 179.245, 179.255; N.J. Rev. Stat. § 2A:164-28; Va. Code §§ 9-192, 19.2-389;

B. Government: Obligations of Processors of Personal Data

1. The First Amendment to the Constitution, as applied by the courts, places limits on government inquiries into and use of information about an individual's political and religious beliefs and affiliations. See, e.g., NAACP v. Alabama, 357 U.S. 449 (1958); Shelton v. Tucker, 364 U.S. 479 (1960); Torcaso v. Watkins, 367 U.S. 488 (1961); Baird v. State Bar of Arizona, 401 U.S. 1 (1971).

2. The Fourth Amendment to the Constitution restricts the means used by the government to collect information from places

in which an individual has "a reasonable expectation of freedom from governmental intrusion." See, e.g., Mancusi v. DeForte, 392 U.S. 364, 368 (1968).

3. The Fourth Amendment, supplemented by the wiretapping and postal statutes, also places strict limits on wiretapping, electronic eavesdropping, access to electronic mail and other computerized records, and the opening of mail by government agencies. 18 U.S.C. §§ 1702, 1703; 18 U.S.C. § 2510, et seq.; 18 U.S.C. § 2701, et seq.; 39 U.S.C. § 3623; Ex Parte Jackson, 96 U.S. 727 (1878); Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967); United States v. U.S. District Court, 407 U.S. 297 (1972).

4. The Fifth Amendment to the Constitution States: It limits the means used by government to collect incriminating information from an individual in a variety of contexts -- from custodial police interrogations to the filing of tax returns -- in addition to limiting the scope of questioning in criminal proceedings themselves. See, e.g., Miranda v. Arizona, 384 U.S. 436 (1966); Marchetti v. United States, 390 U.S. 39 (1968).

5. The equal protection clause of the Fourteenth Amendment to the Constitution (as well as the implicit equal protection requirement of the Fifth Amendment) severely limits government use of "suspect" personal characteristics to adversely classify or penalize individuals. Classifications based on race or national origin are especially suspect and require "strict" judicial scrutiny. Also suspect, but subject to less exacting scrutiny, are classifications based on sex, illegitimacy, and place of citizenship. See, e.g., Brown v. Board of Education, 347 U.S. 483 (1954) (race); Yick Wo v. Hopkins, 118 U.S. 356 (1886) (national origin); Craig v. Boren, 429 U.S. 190 (1976) (sex); Trimble v. Gordon, 430 U.S. 762 (1977) (illegitimacy); Nyquist v. Mauclet, 432 U.S. 1 (1977) (citizenship).

6. Many State Constitutions restrict intrusive collection practices by State governments. See, e.g., Alaska Const. Art. 1, § 22; Ariz. Const. Art. II, § 8; Calif. Const. Art. I, § 1; Fla. Const. Art. 1, § 23; Haw. Const. Art. 1, § 6; Ill. Const. Art. 1, § 6; La. Const. Art. 1, § 5; Mont. Const. Art II, § 10; N.Y. Const. Art. 1, § 12; Pa. Const. Art. 1, § 1; S.C. Const. Art. 1, § 10; Wash. Const. Art. 1, § 7.

7. In addition to the Constitutional restrictions on discrimination by race, national origin, sex, etc., (see entry #5 above), there are numerous specific statutory prohibitions on discriminatory practices by Federal and State governments and entities receiving government funds. See, e.g., 5 U.S.C. §§ 7201-7204; 42 U.S.C. § 2000d.

8. The Privacy Act of 1974 requires that when information is requested from an individual, the collecting agency must provide a detailed notice stating the authorization for and purposes of collection, the extra-agency disclosures ("routine uses") that may be made of the data collected, and the consequences to the individual of failing to provide the information. Personal data must be collected as much as possible directly from the record subject, and information may not ordinarily be collected about an individual's exercise of First Amendment rights (e.g., freedom of expression, assembly, and religion). 5 U.S.C. § 552a.

The Privacy Act also generally prohibits Federal agencies from disclosing personal data except for publicly announced purposes, and requires agencies (1) to keep an accounting of extra-agency disclosures, (2) to instruct record management personnel in the requirements of the Act and the rules for its implementation, and (3) to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records." 5 U.S.C. § 552a.

9. Many State fair information practice statutes limit the type of information that the State government can collect and maintain about individuals. See, e.g., Ark. Stat. § 16-804; Conn. Gen. Stat. § 4-190; Ill. Stat. ch. 116, § 43.5; Mass. Gen. L. ch. 119, § 51E; Mass. Gen. L. ch. 66, § 17A; Ohio Rev. Code § 1347.01; Va. Code § 2.1-377;.

10. Furthermore, statutes in nearly every State limit the ability of government to disclose personal data to third parties. See Ala. Code § 41-8-10; Alaska Stat. § 09.25.140; Ark. Stat. § 16-804; Cal. Civil Code § 1798; Colo. Rev. Stat. § 24-72.204(3)(a); Conn. Gen. Stat. § 4-190; D.C. Code § 37-106.2; Fla. Stat. § 257.261; Ill. Stat. ch. 116, § 43.5; Ill. Stat. ch. 81, § 1202; Ind. Code § 4-1-6; Iowa Code § 68A.7(13); Ky. Rev. Stat. § 61.870; La. Rev. Stat. § 44:13; Me. Rev. Stat. tit. 27, § 121; Me. Rev. Stat. tit. 5, § 1851; Mich. Comp. Laws § 397.603; Minn. Stat. § 13.01; Miss. Code §25-53-53; Mo. Stat. § 182.817; Mont. Rev. Code § 22-1-1103; Neb. Rev. Stat. § 84-712.05; Nev. Rev. Stat. § 239.013; N.J. Rev. Stat. § 18A:73-43.2; N.Y. Civ. Prac. L. & R. § 4509; N.C. Gen. Stat. § 125-19; N.D. Cent. Code 40-38-12; Ohio Rev. Code § 1347.01; Okla. Stat. tit. 74, § 118.17; Or. Rev. Stat. § 192.500(i)(j); Pa. Stat. tit. 24, § 4428; R.I. Gen. Laws § 38-2-2(21; S.C. Code § 60-4-10; S.D. Codified Laws § 14-2-51; Utah Code § 63-50-10; Va. Code § 2.1-342; Wash. Rev. Code § 43.105.040(4); Wis. Stat. § 43:30; Wyo. Stat. § 16-4-203(d).

11. Under the Tax Reform Act of 1976, the Internal Revenue Service may obtain access to certain institutional records about an individual in the hands of certain private recordkeepers only by following notice and challenge procedures similar to those of the Right to Financial Privacy Act of 1978. 26 U.S.C. § 7609.

In addition, the Tax Reform Act strictly limits disclosure of tax returns and return information, and in some cases a court order is required for disclosures to law enforcement agencies for purposes unrelated to tax administration. 26 U.S.C. §§ 6103, 6108.

12. Moreover, most States restrict disclosure of State tax returns and return information. See Alaska Stat. § 9.25.100; Ariz. Rev. Stat. § 43.145; Colo. Rev. Stat. § 39-21-113; Del. Code tit. 30, § 1241; Ga. Code § 48-7-60; Haw. Rev. Stat. § 235.116; Idaho Code § 63-3077; Kan. Stat. § 131.190; Ky. Rev. Stat. § 131.190; La. Rev. Stat. § 47:1508; Me. Rev. Stat. tit. 36, § 5340; Md. Tax Gen. Code §13-202; § 300; Mass. Gen. Laws ch. 62C, §74; Minn. Stat. § 290-611; Neb. Rev. Stat. § 77-27; N.Y. Tax Law § 697; N.C. Gen. Stat. § 105-259; N.D. Cent. Code § 57-38-57; Ohio Rev. Code § 5747.18; Okla. Stat. tit. 68, § 205; Or. Rev. Stat. § 314.835; R.I. Gen. Laws § 44-30-95(c); S.C. Code § 12-35-1530; Tenn. Code § 67-131; Utah Code § 59-1-403; Va. Code § 2.1-342(b); Wash. Rev. Code § 42.17.310; W. Va. Code § 11-21-80; Wis. Stat. § 71.78.

13. The Right to Financial Privacy Act of 1978 generally requires Federal agencies that request access to private financial records either (1) to provide notice of the purpose for which the records are sought and an opportunity for the record subject to challenge disclosure in court, or (2) to obtain a court order for direct access to the records on the basis that notice would allow the record subject to flee or destroy evidence. 12 U.S.C. § 3401, et seq.

Once a Federal agency has obtained an individual's financial records, the Right to Financial Privacy Act ordinarily prohibits that agency from disclosing the records to another one without notifying the individual and obtaining certification from the receiving agency that the records are relevant to a legitimate law enforcement inquiry of the receiving agency. Id.

14. At least eleven States have recently enacted laws, many of them modeled after the Right to Financial Privacy Act, regulating government access to financial records about individuals in the possession of banks, savings and loan associations, or other financial institutions. See Ala. Code § 5-5A-43; Alaska Stat. § 06.05.175; Cal. Gov't Code § 7460; Conn. Gen. Stat. § 36-9j; La. Rev. Stat. § 9:3571; Me. Rev. Stat. Tit. 9-B, § 161; Md. Fin. Inst. Code §1-302; Mass. Gen. Laws ch. 167B, §16; N.H. Rev. Stat. § 359-C; Okla. Stat. tit. 6, §§ 2201 to 2206; Or. Rev. Stat. § 192.550.

15. Under the Federal Fair Credit Reporting Act, consumer reports maintained by consumer reporting agencies may be disclosed to government agencies only in response to a court order or to an agency that requires a consumer report for

legitimate business purposes. 15 U.S.C. § 1681, et seq.

16. Several States have enacted consumer credit reporting statutes which include restrictions on disclosure to government agencies substantially similar to those of the Federal Fair Credit Reporting Act; that is, government access is available only for a legitimate business purpose or in response to a court order. See, e.g., Cal. Civil Code § 1786; Kan. Stat. § 50-703; Me. Rev. Stat. § 1311; Md. Comm. Law Codes § 14-1201; N.H. Rev. Stat. § 359-B; N.Y. Gen. Bus. Law § 380.

17. Under the Cable Communications Policy Act of 1984, a governmental entity may obtain personal data collected by a cable television company about its subscribers only pursuant to a court order finding that the data is likely to reveal criminal activity. Subscribers must be notified and provided with an opportunity to contest the government's claims. 47 U.S.C. § 551(h). Some States also have enacted statutes which restrict the government's ability to obtain access to personal data collected by cable companies about their subscribers. Cal. Penal Code § 637.5; Conn. Gen. Stat. § 53-421; D.C. Code § 43-1845; Ill. Stat. ch. 38, § 87-2; Wis. Stat. § 134.43.

18. The Video Privacy Protection Act of 1988 requires judicial approval before a governmental entity may obtain personal data collected by a video tape sale or rental company about its customers. In some instances, subscribers must be notified and provided with an opportunity to contest the government's request. 18 U.S.C. § 2710.

19. The Privacy Protection Act of 1980 prohibits government agents from conducting unannounced searches of press offices and files if no one in the press office is suspected of a crime. 42 U.S.C. § 2000aa(a). The Act requires instead that the government request voluntary cooperation or subpoena the material sought, giving the holder of the material a chance to contest the action in court. 42 U.S.C. § 2000aa(c). Although the statutory prohibition applies only to searches of media files, the Act directs the U.S. Attorney General to issue guidelines for seeking evidence from other non-suspect third parties, with special consideration to such traditionally confidential relationships as doctor-patient and priest-penitent. 29 C.F.R. §§ 59.1-59.6 (1989).

20. More than half of the States have media shield laws that permit journalists to refuse to identify the sources of information received in the course of professional employment. A number of States also make confidential the information received. Several of the statutes include exceptions in certain limited circumstances, such as criminal proceedings where there is no alternative source of the information and a compelling public interest in having it disclosed. See, e.g., Ariz. Rev. Stat. nn. § 12.2237; R.I. Gen. Laws § 9-19.1-1.

21. Most States have privilege statutes limiting the introduction into legal proceedings of personal information maintained by professionals such as doctors, psychotherapists, attorneys, clergy, and accountants concerning individuals with whom they have a relationship. See Ala. Code tit. 34-26.2; Alaska Stat. §§ 47.30.260, 08.86.200; Ariz. Rev. Stat. § 12-2235; Ark. Stat. §§ 28-607, 72-1616; Cal. Evid. Code § 1010; Colo. Rev. Stat. § 3-90-107; Conn. Gen. Stat. § 52-146; Del. Code tit. § 3518; D.C. Code § 14-307; Fla. Stat. § 90.542; Ga. Code §§ 24-9-21, 43-3-32; Haw. Rev. Stat. § 621.20; Idaho Code §§ 9-203(4), 54-2314; Ill. Stat. ch. 51 §§ 5.1, 5.2; Ind. Code § 34-1-14-5; Iowa Code § 622.10; Ky. Rev. Stat. §§319.111, 421.210, 231.200, 421.215; La. Rev. Stat. §§ 15:476, 37:2366, 13:3734; Me. Rev. Stat. tit. 32, § 3153; Md. Code art. 35, § 13A; Md. Courts Code §§ 9-100, 9-108, 9-109, 9-111; Mich Comp. Laws §§ 338-1018, 600.2156, 600.2157; Minn. Stat. § 595.02; Miss. Code §§ 13-1-21, 73-31-29; Mo. Stat. § 491.060; Mont. Rev. Codes §§ 93-701-4, 66-3212; Neb. Rev. Stat. §§ 27-503 to 27-508; Nev. Rev. Stat. §§ 49.125, 49.215, 49.255; N.H. Rev. Stat. §§ 329:26, 330-A:19; N.J. Rev. Stat. §§ 2A:34A-23, 2A:84A-22.2-9, 45:8B-29; N.Y. Civ. Prac. L. & R. §§ 4504, 4505, 4507, 4508; N.C. Gen. Stat. §§ 8-53.2, 130-184, 130-95; Ohio Rev. Code §§ 4732.9, 2317.02; Okla. Stat. tit. 12, § 385; Okla. Stat. tit. 59, § 1372; Or. Rev. Stat. § 44.040; R.I. Gen. Laws § 9-17-23; S.D. Codified Laws §§ 19-2-3, 19-2-2; Tenn. Code §§ 24-1-206, 24-1-207, 62-143; Tex. Rev. Civ. Stat. art. 3715a; Tex. Rev. Civ. Stat. art. 5561h, § 13(d); Utah Code §§ 58-25-9, 58-35-10, 58-39-10, 78-24-8; Va. Code § 8.01-399; Wash. Rev. Code §§ 18.83.110, 18.53.200, 5.60.050, 5.60.060, 10.52.020; Wis. Stat. §§ 455.09, 885.20, 885.21; Wyo. Stat. §§ 1-139, 33-343.4.

22. At least thirteen States prohibit government employers from requiring a polygraph test as a condition of employment. See, e.g., Conn. Gen. Stat. § 31-51g; Del. Code tit. 19, § 704; D.C. Code § 36-801 to 36-803; Haw. Rev. Stat. § 378.21; La. Rev. Stat. § 37:2848; Me. Rev. Stat. tit. 32, § 7166; Md. Code art. 100, § 95; Mass. Gen. Laws. ch. 149, § 19B; Mich. Comp. Laws § 37.201; N.J. Stat. § 2C:40A-1; N.Y. Labor Law § 733; Or. Rev. Stat. § 659.225; R.I. Gen. Laws § 28-6.1-1. Several States restrict the use of polygraph tests in public employment to law enforcement agencies. See, e.g., Alaska Stat. § 23.10.037; Iowa Code § 730.4; Pa. Cons. Stat. § 7321; Wash. Rev. Code § 49.44.120.

23. The alcoholism and drug abuse confidentiality statutes prohibit government access to treatment records of Federally funded clinics except in a medical emergency, for research or audits, or under a court order. 21 U.S.C. § 1175; 42 U.S.C. § 290dd-3.

Information collected for research or treatment of drug abuse and alcoholism is protected from use for any other

purpose except in a medical emergency or under a court order, and is specifically protected from use against the subject in any criminal proceeding. 21 U.S.C. § 1175; 42 U.S.C. § 290dd-3.

24. Research data collected by the National Centers for Health Services Research and for Health Statistics cannot be disclosed in any way that would identify an individual. 42 U.S.C. § 242m.

25. The Census confidentiality statute absolutely prohibits any use of Census data for other than the original statistical purpose, or any disclosure that would allow an individual to be identified, except to sworn officers and employees of the Census Bureau. 13 U.S.C. § 9.

26. The Family Educational Rights and Privacy Act generally prohibits the use or disclosure of student's records without the consent of the student (or the parent of a minor student). The Act also prohibits government access to personal data in educational records without a court order or lawfully issued subpoena, except for specified education-related purposes. 20 U.S.C. § 1232g.

27. Most States also have enacted statutes which limit the ability of public schools to disclose information from school records to third parties. See, e.g., Ariz. Rev. Stat. § 15-151; Conn. Gen. Stat. § 10-154a; Del. Code tit. 14, § 4111; Fla. Stat. 232.23; Idaho Code § 9-203(6); Ill. Rev. Stat. ch. 122, § 50-1; Iowa Code 22.7; Ky. Rev. Stat. § 421.216; Me. Rev. Stat. tit. 20A, § 6001; Mich. Comp. Laws § 600.2165; Miss. Code § 37-15-3; Mont. Rev. Codes § 93-701-4; N.C. Gen. Stat. § 8-53-4; N.D. Cent. Code § 31-06.1; Ohio Rev. Code 3319.321; Okla. Stat. tit. 70, § 6-115; Or. Rev. Stat. § 336.195; S.D. Codified Laws § 19-2-5.1; Tenn. Code § 10-7-504; Tex. Rev. Civ. Stat. art. 6252-17a, § 3(a)(14); Vt. Stat. tit. 1, § 317(11); Va. Code § 2.1-342(b)(3); Wash. Rev. Code § 42-17.310; Wis. Stat. § 118.125; Wyo. Stat. § 9-692.3(3)(d).

28. The Paperwork Reduction Act of 1980, which is administered by the Office of Management and Budget (OMB), authorizes OMB to refuse to let an agency collect information from the public if another agency has already collected the same information, or if OMB does not believe that the agency either truly needs or can make use of the information. That Act, with certain exceptions, also requires each Federal data collection form to contain a notice telling why the information is being collected, how it is to be used, and whether the individual's response is mandatory, required to obtain a benefit, or voluntary. 44 U.S.C. § 3501, et seq.

29. Nearly every State has statutory limits on the dissemination of criminal justice information. See, e.g., Ala.

Code § 41-9-636; Alaska Stat. § 12.62.010; Cal. Penal Code § 11075-81; Colo. Rev. Stat. § 24-72-301; Conn. Gen. Stat. § 54-142; Del. Code tit. 11, § 8513; Ga. Code § 35-3-34; Haw. Rev. Stat. § 846.1; Ind. Code § 5-2-4; Iowa Code § 692.1; Me. Rev. Stat. tit. 16 § 611; Md. Code art. 27 § 742; Mass Gen. Laws ch. 6, §§ 167-178; Minn. Stat. § 13.82; Mont. Rev. Code § 44-5-101; Neb. Rev. Stat. § 29-3523; N.H. Rev. Stat. § 648.9; N.J. Rev. Stat. § 53:6-18; N.M. Stat. § 15-1A-11; N.C. Gen. Stat. § 114-15; Ohio Rev. Code § 109.57(D); Okla. Stat. tit. 47, § 2-129; S.C. Code § 53-30; Tenn. Code § 10-7-504; Utah Code § 77-59-27; Va. Code §§ 9-192, 19.2-389; Wash. Rev. Code § 43.43.710;.

30. Most States also have statutory provisions for sealing or eliminating certain criminal justice information, such as acquittals or juvenile offenses from an individual's file. Many allow individuals whose records have been so amended to indicate subsequently that they have not been arrested. See, e.g., Ark. Stat. § 5-1109; Cal. Penal Code § 851.8; Colo. Rev. Stat. § 24-72-308; Conn. Gen. Stat. § 54-142a; D.C. Code § 4-131; Del. Code tit. 11, §§ 4371, 8513; Fla. Stat. §§ 901.33, 943.056; Ga. Code § 35-3-37; Haw. Rev. Stat. § 831-3.2; Idaho Code § 19-4807; Ill. Rev. Stat. ch. 127, § 55(a); Ind. Code § 35-4.8; Iowa Code § 692.1; Kan. Stat. nn. § 21-4617; La. Rev. Stat. § 44:9; Md. Code art. 27, §§ 735-741, 292(a); Mass. Gen. Laws ch. 276, § 100A; Mich. Comp. Laws § 28.243; Minn. Stat. § 364.04; Nev. Rev. Stat. § 179.245; N.J. Rev. Stat. §§ 2A:164-28, 2C:52-1; N.M. Stat. § 28-2-3; N.Y. Crim. Proc. Law § 160,.50; Ohio Rev. Code § 2953.43; Or. Rev. Stat. § 137.225; R.I. Gen. Laws § 12-1-12; S.C. Code § 17-4; Tenn. Code § 40-32-101; Utah Code § 77-35-17.5.

C. Government: Data Quality and Security

1. The Privacy Act requires agencies to assure that records used to make a "determination" about an individual are as accurate, relevant, timely, and complete "as is reasonably necessary to assure fairness to the individual." 5 U.S.C. § 552a.

2. As a general safeguard for computerized records and information systems, Federal computer crime statutes and the Electronic Communications Privacy Act of 1986 make it a crime for persons to tamper with computers or access certain computerized records without authorization. 18 U.S.C. §§ 1029, 1030; 18 U.S.C. § 2701, et seq.

3. The Computer Security Act of 1988 requires each Federal agency to provide mandatory training in computer security awareness. Public Law 100-235 § 5.

4. OMB Circular A-71, "Security of Federal Automated Information Systems," mandates security safeguards for unclassified but sensitive Federal records. It spells out each agency's responsibilities for protecting its own files and assigns several agencies to set standards for specific precautions including physical security, personnel screening, and data encryption. (OMB circulars are the equivalent of regulations guiding the behavior of Federal agencies.)

5. More than half of the States require that criminal justice information be reported promptly, completely, and in standard format. Many have quality control requirements for computerized information systems and special requirements that arrest records indicate the disposition of the case. See, e.g., N.D. Cent. Code § 12-60-16; S.C. Code § 73-22.

6. Federal law requires that Federally-funded State and local criminal justice information systems include information on the disposition of any arrest. 42 U.S.C. § 3789g.

7. Most of the State criminal justice information statutes also require strict security measures to protect criminal justice information systems. See, e.g., Alaska Stat. § 12.62.040; Iowa Code § 749B.12.

D. Government: Accountability, Sanctions, and Remedies

(The following are a few provisions applying to laws listed in Parts A, B, and C)

1. Violations of constitutional safeguards, such as those secured by the First, Fourth, and Fifth Amendments, may subject a governmental agency or official to a suit for injunctive or declaratory relief, and/or money damages. A successful plaintiff also may recover court costs and attorney's fees. 42 U.S.C. §§ 1983, 1988.

2. Federal and State courts must exclude illegally obtained evidence from consideration in criminal trials. See United States v. Leon, 468 U.S. 897 (1984); Mapp v. Ohio, 367 U.S. 643 (1961); State v. Novembrino, 105 N.J. 95, 519 A.2d 820 (1987). Courts and other governmental entities must exclude evidence obtained in violation of wiretap statutes. 18 U.S.C. § 2515.

3. The Privacy Protection Act subjects governmental entities who unlawfully conduct searches of press rooms to awards of damages, costs, and attorney's fees. See 42 U.S.C. §2000aa-6.

4. The Privacy Act places accountability for the handling of personal records on the recordkeeping agency and its employees. If an agency violates any provision of the Act and thereby harms an individual, the Act allows the individual to sue the agency for an injunction, damages, and court costs, as appropriate. The Act also provides criminal penalties -- fines of up to $5,000 -- against employees who disclose records in violation of the Act. When an agency hires a contractor to develop or operate a system of Privacy Act records, the contractor assumes the same responsibilities and is subject to the same sanctions as the agency. 5 U.S.C. §§ 552a(g), (i).

5. The Freedom of Information Act provides for persons denied access to government records to sue to compel disclosure. Requestors who prevail in their suits may also obtain awards of costs and attorneys' fees. See 5 U.S.C. § 552.

6. Governmental employers using personal data in violation of the Equal Employment Opportunity Act may be compelled to cease their unlawful conduct and to undertake affirmative actions, such as the reinstatement of employees and payment of backpay. Primary responsibility for enforcing the Act rests with the Equal Employment Opportunity Commission and the U.S. Department of Justice. Aggrieved individuals may sue only if the government does not sue or otherwise resolve the complaint. See 42 U.S.C. § 2000e-5.

7. The Tax Reform Act provides for criminal penalties, including imprisonment, and civil damage awards for unlawfully disclosing tax returns and return information. See 26 U.S.C. §§ 7213, 7431.

8. The Census Confidentiality Statute provides for criminal penalties, including imprisonment, for wrongfully disclosing confidential census data. See 13 U.S.C. § 214.

9. By the terms of the Federal Right to Financial Privacy Act, as a general rule, a customer may challenge a subpoena or formal written request by a government agency to a financial institution for records relating to the customer by filing a motion in Federal district court to quash the subpoena or otherwise prevent disclosure. Court decisions interpreting the statute have concluded that injunctive relief also may be available to prevent disclosure in certain circumstances. Where a government agency obtains or discloses records or information in violation of the Act, the agency or institution is liable to the customer for any actual damages sustained, a $100 penalty, such punitive damages as the court may allow for willful or intentional violation, and court costs and attorney's fees. 12 U.S.C. § 3401, et seq.

10. Enforcement of the Family Educational and Privacy Rights Act is achieved primarily through the right of students and their parents to inspect and challenge education records. Additionally, administrative enforcement of the Act is vested in the Department of Education, and the Act provides for termination of Federal funds if an institution violates the Act and compliance cannot be secured voluntarily. 20 U.S.C. § 1232g.

11. Under the Federal alcohol and drug abuse prevention and treatment statutes, programs that receive Federal Funds are monitored for compliance with the statutes' disclosure restrictions by the State and Federal agencies charged with administrative responsibility for the programs. Violators are subject to a fine. 21 U.S.C. § 1175(f); 42 U.S.C. 290dd-3(f).

E. Private Sector: Rights of Data Subjects

1. Treating disclosures of inaccurate personal information as a form of personal assault, a victim of such inaccurate disclosures may seek redress at common law in a suit for defamation. See W. Prosser, The Law of Torts (5th ed. 1984) at 741-848.

2. Under common law principles of agency and contract law, a person securing the services of bankers, accountants, attorneys, trustees, or physicians is entitled to have these professionals treat his or her communications with them confidentially. See, e.g., Peterson v. Idaho First National Bank, 83 Ida. 578, 367 P.2d 284 (1961); Doe v. Roe, 400 N.Y.S.2d 668 (Sup.Ct. 1977).

3. Privilege statutes in most states require consent for introducing into legal proceedings personal information maintained by professionals such as doctors, psychotherapists, attorneys, clergy, and accountants concerning individuals with whom they have a relationship. See Ala. Code tit. 34-26.2; Alaska Stat. §§ 47.30.260, 08.86.200; Ariz. Rev. Stat. § 12-2235; Ark. Stat. §§ 28-607, 72-1616; Cal. Evid. Code § 1010; Colo. Rev. Stat. § 3-90-107; Conn. Gen. Stat. § 52-146; Del. Code tit. § 3518; D.C. Code § 14-307; Fla. Stat. § 90.542; Ga. Code §§ 24-9-21, 43-3-32; Haw. Rev. Stat. § 621.20; Idaho Code §§ 9-203(4), 54-2314; Ill. Stat. ch. 51 §§ 5.1, 5.2; Ind. Code § 34-1-14-5; Iowa Code § 622.10; Ky. Rev. Stat. §§319.111, 421.210, 231.200, 421.215; La. Rev. Stat. §§ 15:476, 37:2366, 13:3734; Me. Rev. Stat. tit. 32, § 3153; Md. Code art. 35, § 13A; Md. Courts Code §§ 9-100, 9-108, 9-109, 9-111; Mich. Comp. Laws §§ 338-1018, 600.2156, 600.2157; Minn. Stat. § 595.02; Miss. Code §§ 13-1-21, 73-31-29; Mo. Stat. § 491.060;

Mont. Rev. Codes §§ 93-701-4, 66-3212; Neb. Rev. Stat. §§ 27-503 to 27-508; Nev. Rev. Stat. §§ 49.125, 49.215, 49.255; N.H. Rev. Stat. §§ 329:26, 330-A:19; N.J. Rev. Stat. §§ 2A:34A-23, 2A:84A-22.2-9, 45:8B-29; N.Y. Civ. Prac. L. & R. §§ 4504, 4505, 4507, 4508; N.C. Gen. Stat. §§ 8-53.2, 130-184, 130-95; Ohio Rev. Code §§ 4732.9, 2317.02; Okla. Stat. tit. 12, § 385; Okla. Stat. tit. 59, § 1372; Or. Rev. Stat. § 44.040; R.I. Gen. Laws § 9-17-23; S.D. Codified Laws §§ 19-2-3, 19-2-2; Tenn. Code §§ 24-1-206, 24-1-207, 62-143; Tex. Rev. Civ. Stat. art. 3715a; Tex. Rev. Civ. Stat. art. 5561h, § 13(d); Utah Code §§ 58-25-9, 58-35-10, 58-39-10, 78-24-8; Va. Code § 8.01-399; Wash. Rev. Code §§ 18.83.110, 18.53.200, 5.60.050, 5.60.060, 10.52.020; Wis. Stat. §§ 455.09, 885.20, 885.21; Wyo. Stat. §§ 1-139, 33-343.4.

4. The use of eavesdropping technology, the opening of mail, and the interception of electronic mail, radio communications, data transmissions, and telephone calls are prohibited without consent. 18 U.S.C. § 2510, et seq.; 39 U.S.C. § 3623; 47 U.S.C. § 605.

5. Most states also have statutes requiring consent for electronic eavesdropping and interception of communications by wire or radio. See, e.g., Alaska Stat. § 11.60.290; Ariz. Rev. Stat. § 13:1051; Cal. Penal Code § 631; Colo. Rev. Stat. § 18-9-301; Del. Code tit. 11, § 1335; Fla. Stat. § 934.01; Ga. Code § 16-11-62; Haw. Rev. Stat. § 711-1111; Idaho Code § 18-6701; Kan. Stat. § 22-2514; Ky. Rev. Stat. § 526.010; La. Rev. Stat. § 14:322; Me. Rev. Stat. tit. 15, § 709; Md. Cts. & Jud. Proc. Code § 10-401; Mich. Comp. Laws § 750-539; Minn. Stat. § 626A.01; Neb. Rev. Stat. § 86-701; Nev. Rev. Stat. § 200.610; N.H. Rev. Stat. § 570-A:1; N.J. Rev. Stat. § 2A:156A-1; N.M. Stat. § 30-12-2; N.Y. Crim. Proc. Law § 700.05; Ohio Rev. Code § 2933.58; Pa. Cons. Stat. § 5701; S.D. Compiled Laws § 23-13A-1; Tex. Rev. Stat. Penal Code § 16.02; Utah Code § 77-54(A)-1; Va. Code § 19.2-61; Wash. Rev. Code § 9.73.030; Wis. Stat. § 968.27.

6. Under the Employee Polygraph Protection Act of 1988, employees may generally refuse to take a polygraph test as a condition of original or continued employment without risking discipline or some other adverse employment action. 29 U.S.C. § 2001, et seq.

7. Many State laws also restrict the use of mandatory polygraph tests as a condition for employment. See, e.g., Alaska Stat. § 23.10.37; Cal. Labor Code § 432.2; Conn. Gen. Stat. § 31-51g; Del. Code tit. 19, § 704; D.C. Code §§ 36-801 to 36-803; Haw. Rev. Stat. § 378.21; Idaho Code §44-903; Iowa Code § 730.4; La. Stat. § 37:2848; Me. Rev. Stat. tit. 32,

§ 7166; Md. Code art. 100, § 95; Mass. Gen. Laws ch. 149, § 19B; Mich. Comp. Laws § 37.201; Minn. Stat. § 181.75; Mont. Rev. Codes § 39.2-304; N.J. Stat. § 2C:40A-1; N.Y. Labor Law § 733; Or. Rev. Stat. § 659.225; Pa. Cons. Stat. § 7321; R.I. Gen. Laws § 28-6.1.1; Tex. Rev. Civ. Stat. art. 4413(29cc); Utah Code § 34-37-16; Ver. Stat. § 5a; W.Va. Code § 21-5-5a; Wis. Stat. § 111.37.

8. Under the Cable Communications Policy Act of 1984, subscribers are entitled to annual notification from their cable television companies about the nature of personal data collected, data disclosure practices, and subscriber rights to inspect and correct errors in such data. Without prior consent by a subscriber, a cable TV company may not use the cable system to collect personal information about its subscribers and generally may not disclose such data. 47 U.S.C. § 551.

9. Some States also have enacted cable television privacy statutes which permit subscribers to correct information or have their names deleted from data files maintained by cable operators. See, e.g., Cal. Penal Code § 637.5; Ill. Stat. ch. 38, § 87-2. A number of State statutes prohibit disclosure of personal information collected by a cable operator unless the subscriber has notice and has not objected to the disclosure. See, e.g., Cal. Penal Code § 637.5; Conn. Gen. Stat. § 53422; Ill. Stat. ch. 38, § 87-2; Wis. Stat. § 134.43.

10. The Video Privacy Protection Act of 1988 prohibits video tape sale or rental companies from disclosing personal data about customers without their consent or court approval. In most instances, subscribers must be notified and provided with an opportunity to contest the data requests prior to a judicial determination. Video tape companies may disclose customer names and addresses, and the subject matter (but not titles) of their purchases or rentals if for direct marketing use, only after notifying them of their right to prohibit such disclosures. 18 U.S.C. § 2710. Some State video privacy laws contain broader proscriptions, barring, for example, the disclosure of customer names and addresses or of subject matter of purchases or rentals without the customer's consent. See, e.g., Cal. Civil Code § 1799.3.

11. The Fair Credit Reporting Act requires that, if a consumer report is used in any decision to deny credit, insurance or employment, the report user must tell the consumer the name and address of the reporting agency. The Act also provides for access and correction procedures. 15 U.S.C. §1681.

12. The Equal Credit Opportunity Act requires that, when credit is denied or revoked, the applicant must be either notified of the reasons for the decision or informed of his right to learn the reasons. 15 U.S.C. § 1691; 12 C.F.R. § 202.9 (1990).

13. The Fair Credit Billing Act requires creditors, on request, to investigate alleged billing errors and to provide documentary evidence of the individual's indebtedness. While investigating a dispute, the creditor is prohibited from taking action against the individual with respect to the disputed debt. 15 U.S.C. § 1666; 12 C.F.R. § 226.13 (1990).

14. A number of State statutes prohibit financial institutions from disclosing a customer's financial records without either the customer's consent or a subpoena. See, e.g., Ill. Rev. Stat. ch. 16 1/2, § 148.1; Me. Rev. Stat. § 16; Md. Fin. Inst. Code §1-302. Mass. Gen. Laws ch. 167B, §16; Okla. Stat. tit. 6, § 2201 to 2206; Or. Rev. Stat. § 192.550.

15. The Employee Retirement Income Security Act allows employees to find out the total of their accrued retirement benefits, and either the amount that is nonforfeitable or the date on which any benefits will become nonforfeitable. 29 U.S.C. § 1025.

16. Provisions of the Uniform Commercial Code, enacted in all States, encourage disclosure to the customer of the bank's record of a transaction as soon as possible after it is consummated, in order to limit the bank's liability for errors. Only after the customer is informed of the bank's version of what has occurred can he be held responsible for failing to discover and dispute errors. See, e.g., Tenn. Code § 47-4-406.

17. Under the Electronic Funds Transfer Act, customers with electronic funds transfer (EFT) accounts are entitled to regular disclosures from their banks. The bank must make extensive disclosures to customers about specific EFT transactions, both at the time they are made and in the form of periodic statements. In addition, customers must be notified, at the time they contract for EFT services, of their rights, liabilities, charges, procedures, etc., connected with the services, and of whom to contact if an unauthorized transfer is suspected. In the case of preauthorized periodic transfers -- such as automatic bill paying -- the bank must provide either positive or negative notice as to whether payments are being made on schedule. The Act also sets up detailed procedures for the resolution of any inaccuracies in customer accounts, and imposes liability on the bank for errors in the transmission or documentation of transfers. 15 U.S.C. § 1693; 12 C.F.R. Part 205 (1990).

18. Many States have statutes allowing individuals to see and have a copy of their medical records. See, e.g., Cal. Health & Safety Code § 25250; Colo. Rev. Stat. § 25-1-801; Conn. Gen. Stat. § 4-105; Fla. Stat. §§ 455.241, 395.017; Ind. Stat. § 34-3-15.5-4; La. Rev. Stat. § 40:2014.1; Mass. Gen. Laws ch. 111 § 70E; Minn. Stat. § 144.335; Nev. Rev. Stat. § 629.061; Okla. Stat. tit. 76, § 19; R.I. Gen. Laws § 5-37.3.3; Tenn. Code § 53-1322; Va. Code § 8.01-413; Wisc. Stat. § 146.83.

19. Some states have enacted statutes which require the patient's consent for disclosure of medical records. See, e.g., Alaska Stat. § 47.30.260; Cal. Civil Code § 56; Fla. Stat. §§ 455.241, 395.017; Nev. Rev. Stat. § 49.215-245.

20. Under the Family Educational Rights and Privacy Act, students and their parents may inspect and challenge the accuracy and completeness of education records maintained about the students in schools that receive public funding. Additionally, the Act requires that students and their parents be informed of their statutory rights under the Act. 20 U.S.C. § 1232g.

21. Some State statutes permit students and their parents to inspect and challenge the accuracy and completeness of school records. See, e.g., Cal. Educ. Code § 49060; Del. Code tit. 14, § 4111.

22. Some State statutes allow individuals access to personnel records about them held by their employer. See, Cal. Lab. Code § 1198.5; Conn. Gen. Stat. § 31-128a; Del. Code tit. 19, § 723; Ill. Stat. ch. 48, § 2001; Me. Rev. Stat. tit. 26, § 631; Mass. Gen. Laws ch. 149, § 52C; Mich. Comp. Laws § 423.501; Nev. Rev. Stat. § 613.075; N.H. Rev. Stat. § 275.56; Ohio Rev. Code § 4113.23; Or. Rev. Stat. § 652.750; Pa. Stat. tit. 43, § 1321; R.I. Gen. Laws § 28-6.4-1; S.D. Codified Laws § 3-6A-31; Wash. Rev. Code 49.12.250.

23. The NAIC Model Law (enacted in 13 States) requires insurers to provide general information about their personal data practices to applicants and policyholders, with further information available on request. Individuals who are denied insurance are entitled to learn the specific reasons and information used in refusing coverage. Applicants or policyholders may obtain access to non-privileged personal information about them, and may propose that such information be corrected, amended, or deleted. When information is collected through personal interviews with an individual's neighbors, acquaintances, or associates, the individual is entitled to a copy of the resulting report and a personal

interview in connection with it. Finally, the Model Law imposes data quality standards on underwriting decisions by prohibiting denials of coverage based solely on previous denials of coverage. See, e.g., Calif. Ins. Code § 791.

F. Private Sector: Obligations of Processors of Personal Data

1. The limits set by the common law on invasion of property rights (for example, in the law of trespass) have by implication limited the manner in which information may be collected about an individual. In the last century or so, a distinct right of action for invasion of privacy or intrusion on solitude has been recognized by courts in virtually all States. A trespass on property is not required in order to establish liability for intrusion; damages may be collected for a variety of intrusions into places or affairs as to which the individual has a reasonable expectation of privacy. W. Prosser, The Law of Torts (5th ed. 1984) at 854-56.

At common law in virtually all States, an individual may sue for damages suffered from an objectionable public disclosure of private facts. W. Prosser, The Law of Torts (5th ed. 1984) at 856-63.

Liability for defamation at common law may be imposed on a person who discloses inaccurate information about another unless the defense of "qualified privilege" is recognized by the court, applies to the defendant, and has not been abused by him. Although most States have applied the privilege broadly in cases concerning disclosures of personal information in the normal course of business, they have historically varied as to the type of conduct that constitutes an abuse of privilege. W. Prosser, The Law of Torts (5th ed. 1984) at 832-35.

2. Under common law principles of agency and contract law recognized in most States, duties of confidentiality are considered to be owed by various categories of professionals and others performing services for an individual, including bankers, accountants, attorneys, trustees, and physicians. See, e.g., Peterson v. Idaho First National Bank, 83 Ida. 578, 367 P.2d 284 (1961); Doe v. Roe, 400 N.Y.S.2d 668 (Sup. Ct. 1977).

3. Moreover, at common law, banks have a duty to maintain the confidentiality of bank records. See, e.g., Brex v. Smith, 104 N.J. Eq. 386, 390, 146 A. 34, 36 (1929); Sparks v. Union Trust Co. of Shelby, 256 N.C. 478, 124 S.E.2d 365, 367 (1962); Suburban Trust Co. v. Waller, 44 Md.App. 335, 408 A.2d 758

(1979); Milohnich v. First Nat'l Bank of Miami Springs, 224 So. 2d 284 (Fla. 1969); Peterson v. Idaho First Nat'l Bank, 83 Idaho 578, 367 P.2d 284 (1961). The common law duty to maintain confidentiality of bank records is supplemented by a number of State statutes which also restrict disclosures by financial institutions of information they have on their customers. See, e.g., Alaska Stat. § 06.30.120; Conn. Gen. Stat. § 36-9j; Ill. Rev. Stat. ch. 16 1/2, § 148.1; Iowa Code § 527.10; La. Rev. Stat. § 9:3571; Me. Rev. Stat. § 161; Md. Fin. Inst. Code §1-302; Mass. Gen. Laws ch. 167B, §16; Okla. Stat. tit. 6, §§ 2201-2206; Or. Rev. Stat. § 192.550;

4. Under privilege statutes in most states, there are limits on introducing into legal proceedings, personal information maintained by professionals such as doctors, psychotherapists, attorneys, clergy, and accountants concerning individuals with whom they have a relationship. See Ala. Code tit. 34-26.2; Alaska Stat. §§ 47.30.260, 08.86.200; Ariz. Rev. Stat. § 12-2235; Ark. Stat. §§ 28-607, 72-1616; Cal. Evid. Code § 1010; Colo. Rev. Stat. § 3-90-107; Conn. Gen. Stat. § 52-146; Del. Code tit. § 3518; D.C. Code § 14-307; Fla. Stat. § 90.542; Ga. Code §§ 24-9-21, 43-3-32; Haw. Rev. Stat. § 621.20; Idaho Code §§ 9-203(4), 54-2314; Ill. Stat. ch. 51 §§ 5.1, 5.2; Ind. Code § 34-1-14-5; Iowa Code § 622.10; Ky. Rev. Stat. §§319.111, 421.210, 231.200, 421.215; La. Rev. Stat. §§ 15:476, 37:2366, 13:3734; Me. Rev. Stat. tit. 32, § 3153; Md. Code art. 35, § 13A; Md. Courts Code §§ 9-100, 9-108, 9-109, 9-111; Mich Comp. Laws §§ 338-1018, 600.2156, 600.2157; Minn. Stat. § 595.02; Miss. Code §§ 13-1-21, 73-31-29; Mo. Stat. § 491.060; Mont. Rev. Codes §§ 93-701-4, 66-3212; Neb. Rev. Stat. §§ 27-503 to 27-508; Nev. Rev. Stat. §§ 49.125, 49.215, 49.255; N.H. Rev. Stat. §§ 329:26, 330-A:19; N.J. Rev. Stat. §§ 2A:34A-23, 2A:84A-22.2-9, 45:8B-29; N.Y. Civ. Prac. L. & R. §§ 4504, 4505, 4507, 4508; N.C. Gen. Stat. §§ 8-53.2, 130-184, 130-95; Ohio Rev. Code §§ 4732.9, 2317.02; Okla. Stat. tit. 12, § 385; Okla. Stat. tit. 59, § 1372; Or. Rev. Stat. § 44.040; R.I. Gen. Laws § 9-17-23; S.D. Codified Laws §§ 19-2-3, 19-2-2; Tenn. Code §§ 24-1-206, 24-1-207, 62-143; Tex. Rev. Civ. Stat. art. 3715a; Tex. Rev. Civ. Stat. art. 5561h, § 13(d); Utah Code §§ 58-25-9, 58-35-10, 58-39-10, 78-24-8; Va. Code § 8.01-399; Wash. Rev. Code §§ 18.83.110, 18.53.200, 5.60.050, 5.60.060, 10.52.020; Wis. Stat. §§ 455.09, 885.20, 885.21; Wyo. Stat. §§ 1-139, 33-343.4.

5. The wiretapping and postal statutes and the Communications Act of 1984 generally prohibit the use of eavesdropping technology, the opening of mail, and the interception of electronic mail, radio communications, data transmissions, and telephone calls without consent. 18 U.S.C. § 2510, et seq.; 39 U.S.C. § 3623; 47 U.S.C. § 605.

6. Most States also restrict electronic eavesdropping and interception of communications via wire or radio. See Ala. Code tit. 13A, § 11.30; Alaska Stat. § 11.60.290; Ariz. Rev. Stat. § 13:1051; Ark. Stat. § 73-1810; Cal. Penal Code §§ 631 to 637; Colo. Rev. Stat. §§ 18-9-301, 16-15-101; Conn. Gen. Stat. 54-41a; Del. Code tit. 11, § 1335; D.C. Code § 23:541; Fla. Stat. § 934.01; Ga. Code §16-11-62; Haw. Rev. Stat. § 711-1111; Idaho Code § 18-6701; Ill. Rev. Stat. ch. 134, § 15a; Iowa Code § 716.7-8; Kan. Stat. § 22-2514; Ky. Rev. Stat. § 526.010; La. Rev. Stat. § 14:322; Me. Rev. Stat. tit. 15, § 709; Md. Cts. & Jud. Proc. Code § 10-401; Mass. Gen. Laws ch. 272, § 99; Mich. Comp. Laws § 750-539; Minn. Stat. § 626A.01; Neb. Rev. Stat. § 86-701; Nev. Rev. Stat. § 200.610; N.H. Rev. Stat. § 570-A:1; N.J. Rev. Stat. § 2A:156A-1; N.M. Stat. § 30-12-2; N.Y. Crim. Proc. Law § 700.05; N.C. Gen. Stat. § 14-155; N.D. Cent. Code § 12.1-15-02; Ohio Rev. Code § 2933.58; Pa. Cons. Stat. § 5703; R.I. Gen. Laws § 12-35-21; S.D. Codified Laws § 23-13A-1; Tenn. Code 39-3-1324; Tex. Rev. Stat. Penal Code 16.02; Utah Code § 77-54(A)-1; Va. Code § 19.2-61; Wash. Rev. Code § 9.73.030; W. Va. Code § 61-3-246; Wis. Stat. § 968.27.

7. As a general safeguard for computerized records and information systems, Federal computer crime statutes and the Electronic Communications Privacy Act of 1986 make it a crime for persons to tamper with computers or access certain computerized records without authorization, or for providers of electronic communications services to disclose the contents of stored communications. 18 U.S.C. §§ 1029, 1030; 18 U.S.C. § 2701, et seq.

8. The Employee Polygraph Protection Act of 1988 generally prohibits employers from requiring a polygraph test as a condition of employment or using the results of such tests as the sole basis for disciplining the employee or taking some other adverse employment action. Except pursuant to a court order or when informing the government of criminal conduct, employers are barred from publicly disclosing the results of polygraph tests. 29 U.S.C. § 2001, et seq.

9. At least 17 States also prohibit an employer from requiring a polygraph test as a condition of original or continued employment. See, e.g., Alaska Stat. § 23.10.37; Cal. Labor Code § 432.2; Conn. Gen. Stat. § 31-51g; Del. Code tit. 19, § 704; D.C. Code §§ 36-801 to 36-803; Haw. Rev. Stat. § 378.21; Idaho Code § 44-903; Iowa Code § 730.4; La. Stat. § 37:2848; Me. Rev. Stat. tit. 32, § 7166; Md. Code art. 100, § 95; Mass. Gen. Laws ch. 149, § 19B; Mich. Comp. Laws § 37.201; Minn. Stat. § 181.75; Mont. Rev. Codes § 39.2-304; N.J. Stat. § 2C:40A-1; N.Y. Labor Law § 733; Or. Rev. Stat.

§ 659.225; Pa. Cons. Stat. § 7321; R.I. Gen. Laws § 28-6.1.1; Tex. Rev. Civ. Stat. art. 4413(29cc); Utah Code § 34-37-16; Ver. Stat. § 5a; W.Va. Code § 21-5-5a; Wis. Stat. § 111.37.

10. The Federal Equal Employment Opportunity Act and supplementary laws in virtually every State prohibit employment discrimination on the basis of race, sex, religion, national origin, and a variety of other characteristics. 42 U.S.C. § 2000e, et seq.

Over half the States add to Federal protections by generally prohibiting employers from collecting information about job applicant's race, sex, color, religion, national origin, and other attributes. See, e.g., Colo. Rev. Stat. § 24-24-301, et seq.; Hawaii Rev. Stat. § 378-1, et seq.

11. The Federal fair housing statute generally prohibits discrimination in the sale, rental, or financing of residential housing. 42 U.S.C. §§ 3604, 3605.

12. Under the Cable Communications Policy Act of 1984, a cable TV company may not use the cable system to collect personal information and generally may not use or disclose such data about its subscribers without prior subscriber consent. 47 U.S.C. § 551. A number of State cable statutes prohibit cable operators from disclosing data about subscribers unless the subscriber has notice and has not objected to the disclosure. See Cal. Penal Code § 637.5; Conn. Gen. Stat. § 53-422; Ill. Stat. ch. 38, § 87-2; Wis. Stat. § 134.43.

13. The Video Privacy Protection Act of 1988 generally prohibits videotape sale or rental companies from disclosing personal data about customers without their consent. A customer's name and address (and subject matter of their purchases or rentals if for direct marketing use) may be disclosed if, after notifying the customer of her right to prohibit such disclosures, she does not object. 18 U.S.C. § 2710. Several States have video privacy laws that are similar to the Federal statute. See, e.g., Cal. Civil Code § 1799.3; Del. Code tit. 11, § 925.

14. The Fair Credit Reporting Act requires that, when a data broker is hired to prepare an "investigative consumer report" (an investigation into the consumer's "character, general reputation, personal characteristics, or mode of living" by means of interviews with friends, neighbors, and associates), the request for information must be disclosed to the subject of the report, who is then entitled to learn the nature and scope of the inquiry requested. 15 U.S.C. § 1681d.

Under the Federal Fair Credit Reporting Act, consumer reports maintained by consumer reporting agencies may be disclosed without consent only for legitimate business purposes or pursuant to a court order. 15 U.S.C. § 1681b.

15. The Equal Credit Opportunity Act regulates the manner in which information collected by creditors may be used in making decisions regarding the extension of credit. Certain information may not be collected at all. Other information may be collected by a creditor for limited purposes but may not be used for prohibited purposes. 15 U.S.C. 1691, et seq.

The regulations implementing the Equal Credit Opportunity Act impose limits on the type of information that can be collected by a creditor, prohibiting inquiries into a credit applicant's sex, race, color, religion, or marital status, except for strictly limited purposes. The rules proscribe the retention and preservation of certain information by creditors while also requiring the preservation of certain specified records relating to credit transactions. 15 U.S.C. § 1691, et seq.; 12 C.F.R. Part 202 (1990).

16. At least 32 States have enacted equal credit opportunity statutes that generally prohibit the collection by creditors of such information as race, religion, or sex. See e.g., Ky. Rev. Stat. § 344.370; Wash. Rev. Code § 49.60.175.

17. The Fair Debt Collection Practices Act strictly limits the communications that debt collection agencies may make about the debtors whose accounts they are attempting to collect. 15 U.S.C. § 1692, et seq.

18. The Electronic Funds Transfer Act explicitly requires regular disclosures to customers with electronic funds transfer (EFT) accounts. The bank must make extensive disclosures to customers about specific EFT transactions, both at the time they are made and in the form of periodic statements. In addition, customers must be notified, at the time they contract for EFT services, of their rights, liabilities, charges, procedures, etc., connected with the services, and of whom to contact if an unauthorized transfer is suspected. In the case of preauthorized periodic transfers -- such an automatic bill paying -- the bank must provide either positive or negative notice as to whether payments are being made on schedule. The Act also sets up detailed procedures for the resolution of any inaccuracies in customer accounts, and imposes liability on the bank for errors in the transmission or documentation of transfers. 15 U.S.C. § 1693; 12 C.F.R. Part 205.

19. Federal statutes prohibit the unauthorized use or disclosure of alcoholism and drug abuse treatment records by private clinics receiving Federal funds, except in a medical emergency, for research or audits, or under a court order. 21 U.S.C. § 1175; 42 U.S.C. § 290dd-3.

20. Virtually every State has statutes that limit the use and disclosure of medical or mental health records. See, e.g., Cal. Civ. Code § 56; Colo. Rev. Stat. § 18-4-412; Conn. Gen. Stat. § 52-146h; Ill. Stat. ch. 91 1/2. § 801: Mass. Gen. Laws ch. 111, § 70E; N.M. Stat. § 42-1-15. Pa. Stat. tit. 50, § 7111; R.I. Gen. Laws § 5-37.3.3; Tenn. Code § 10-7-504; Tex. Rev. Civ. Stat. art. 4447d; Wis. Stat. § 146.82.

21. The Family Educational Rights and Privacy Act provides that schools receiving public funds are prohibited from using or disclosing a student's records without the consent of the student (or the parent of a minor student) except for certain specified purposes, or pursuant to a court order or lawfully issued subpoena. 20 U.S.C. § 1232g.

22. Some States also have enacted statutes which place limitations on the ability of schools to disclose information from school records to third parties. See, e.g., Del. Code tit. 14, § 4111; Idaho Code § 9-203(6); Ky. Rev. Stat. § 421.216; Mich. Comp. Laws § 600.2165; N.C. Gen. Stat. § 8-53-4.

23. The NAIC Model Law (approved by the NAIC in December 1979 and enacted in 13 States since then) requires insurance companies and insurance agents to notify applicants about the collection and disclosure of personal data, and to specify when information is requested solely for marketing or research purposes. In addition, the Model Law restricts the use of "pretext interviews" (in which the identity or purpose of the interviewer is misrepresented) and requires specific consent forms to be used for the collection of information that requires authorization from an individual. A specific notice must also be given if information is collected via personal interviews with neighbors, acquaintances, or associates of an individual. See, e.g., Calif. Ins. Code § 791.

Finally, under the NAIC Model Law, an insurance company or insurance agent may disclose information only under the circumstances specified by the Law or with the individual's consent. See, e.g., Ill. Stat. ch. 73, §§ 1001-1024.

G. Private Sector: Data Quality and Security

1. As a general safeguard for computerized records and information systems, Federal computer crime statutes and the Electronic Communications Privacy Act of 1986 make it a crime for persons to tamper with computers or access certain computerized records without authorization, or for providers of electronic communication services to disclose the contents of stored communications. 18 U.S.C. §§ 1029, 1030; 18 U.S.C. § 2701, et seq.

2. Almost all States also have criminalized similar conduct through enactment of computer crime or stored communications statutes. See, e.g., Ala. Code § 13A-8-101; Alaska Stat. §§ 11.81.900(b)(44), 11.46.200(a); Ariz. Rev. Stat. §§ 13-2301E, 13-2316; Cal. Penal Code § 502; Colo. Rev. Stat. § 18-5.5-101; Conn. Gen. Stat. § 53a-250; Del. Code tit. 11, §§ 931 to 939; Fla. Stat. §§ 815.01, 934.21, et seq.; Ga. Code § 16-9-90; Haw. Rev. Stat. §§ 708-890, 803-47.5; Idaho Code § 18-22; Ill. Rev. Stat. ch. 38, § 16-9; Ind. Code § 35-43-1-4; Iowa Code § 716A; Kan. Stat. § 21-3755; Ky. Rev. Stat. § 434; La. Rev. Stat. § 14:73.1; Md. Cts. & Jud. Proc. § 10-4A-01, et seq.; Mass. Gen. Laws ch. 266, § 30(2); Mich. Comp. Laws ch. 266, § 752.791; Minn. Stat. §§ 609.87, 626A.26, et seq; Miss. Code § 97-45-1; Mo. Stat. § 569.093; Mont. Code § 45-6-310; Neb. Rev. Stat. §§ 28-1343, 86-707.09; Nev. Rev. Stat. § 205.473; N.H. Rev. Stat. § 638:16; N.J. Rev. Stat. §§ 2A:38A-1, 2C:20-1; N.M. Stat. § 30-16A-1; N.Y. Penal Law § 156; N.C. Gen. Stat. § 14-453; N.D. Cent. Code § 12.1-06.1-08; Ohio Rev. Code §§ 2901.01, 2913.01; Okla. Stat. tit. 21, §§ 1951 to 1956; Or. Rev. Stat. §164.377; Pa. Stat. tit. 18, §§ 3933, 5471, et seq.; R.I. Gen. Laws § 11-52-1; S.C. Code § 16-16-10; S.D. Codified Laws § 43-43B-7; Tenn. Code § 39-3-14-4; Tex. Penal Code §§ 16.04, 33.01; Tex. Crim. Proc. Code Art. 18.21; Utah Code §§ 76-6-701, 77-23b, et seq.; Va. Code § 18.2-152.1; Wash. Rev. Code § 9A.48.100; Wis. Stat. § 943.70; Wyo. Stat. § 6-3-501.

3. The Fair Credit Reporting Act regulates the quality of data used by reporting agencies, requiring "reasonable procedures" to avoid reporting specified categories of obsolete information and to verify information in investigative consumer reports that are used more than once. It also requires brokers to maintain "reasonable" security procedures, including procedures to verify the identity and stated purposes of recipients of consumer reports. 15 U.S.C. § 1681, et seq.

H. Private Sector: Accountability, Sanctions, and Remedies

(The following are a few provisions applying to laws listed in Parts E, F, and G.)

1. The common law provides redress for successful plaintiffs who bring suit for invasion of privacy. Typically, the individual may recover money damages for injury to emotions and mental suffering. Wood v. Hustler Magazine, Inc. 736 F.2d 1084 (5th Cir. 1984), reh'g denied 744 F.2d 94, cert. denied 469 U.S. 1107 (1984). Recovery of punitive damages is also possible, Cantrell v. Forest City Pub. Co., 419 U.S. 245 (1974); and in certain circumstances, injunctive relief may be available. Zacchini v. Scripps-Howard Broadcasting Co, 433 U.S. 562 (1976).

At common law, plaintiffs also may bring suit for defamation of character and recover for general damages, including impairment of reputation, Dalton v. Meister, 52 Wis.2d 173, 188 N.W.2d 494 (1971), cert. denied 405 U.S. 934 (1971), and mental anguish and suffering. Time, Inc. v. Firestone, 424 U.S. 448 (1976). In addition, special damages may be recovered to enhance general damages. Snowden v. Pearl River Broadcasting Corp., 251 So.2d 405 (1971). Punitive damages also may be awarded for malicious defamatory publications, and in some cases nominal damages are available. Conrad v. Dillingham, 23 Ariz. 529, 206 P.2d 166 (1922). Injunctive relief, however, is rarely granted in defamation actions. Near v. Minnesota, 283 U.S. 697 (1931).

2. At common law, a depositor may recover damages from a financial institution for an unauthorized disclosure of financial information on the depositor. See, e.g., Suburban Trust Co. v. Waller, 44 Md. App. 335, 408 A.2d 758 (1979).

3. Financial institutions that violate state statutes restricting disclosure of customer records are frequently subject to criminal and civil penalties. See, e.g., Md. Fin. Inst. Code § 1-305; Mass. Gen. Laws ch. 167B, § 20; Conn. Gen. Stat. §§ 36-9n, 53a-42; Or. Rev. Stat. § 192.590.

4. Fiduciary relationship between accountants and clients make extra-judicial disclosure of information obtained in the course of that relationship an actionable tort. See, e.g., Wagerheim v. Alexander Grant & Co., 19 Ohio App. 3d 7, 482 N.E.2d 955 (1983).

5. An attorney who discloses a confidence or a secret of the attorney's client may be publicly censured and convicted of contempt. See, e.g., In the Matter of Ronald C. Wyse, 212 Mont. 339, 688 P.2d 758 (1984).

6. Patients may recover damages from physicians for unauthorized disclosures concerning patients on the grounds that such disclosures constitute an actionable invasion of privacy and a breach of the privileged relationship. See, e.g., Humphers v. First Interstate Bank, 298 Or. 706, 696 P.2d 527 (1985); Stempler v. Speidell, 100 N.J. 368, 495 A.2d 857 (1985).

7. Federal wiretapping, computer crime, and postal statutes subject persons unlawfully tampering with computers, accessing electronic mail or other computerized records, opening mail, or engaging in electronic eavesdropping, to criminal prosecution, civil damage awards, or both. See 18 U.S.C. §§ 1029, 1030, 1702, 1703, 2511, 2520, 2701, 2707.

Under their own wiretapping and computer crime statutes, most States also subject persons engaging in such conduct to criminal penalties, civil damages, or both. See e.g., Cal. Penal Code §§ 631, 632, 637.2; Md. Cts. & Jud. Proc. Code §§ 10-402, 10-410, 10-4A-02, 10-4A-08.

8. Employers that violate the Employee Polygraph Protection Act of 1988 may be subject to a fine of up to $10,000, injunctive relief such as employee reinstatements, and awards of damages, costs, and attorneys fees. Some States subject employers who use polygraph tests to criminal prosecution. See, e.g., Conn. Gen. Stat. § 31-51g; Or. Rev. Stat. § 659.225; Pa. Cons. Rev. Stat. § 7321.

9. Cable television companies that violate subscriber privacy provisions of the Cable Communications Policy Act of 1984 may be liable for actual damage awards of at least $1,000, punitive damages, costs, and attorneys fees. 47 U.S.C. § 551(f). In addition, under several State cable statutes, cable companies that violate privacy provisions are subject to civil and criminal penalties. See, e.g., Cal. Penal Code § 837.5; Conn. Gen. Stat. § 53-422; Ill. Stat. ch. 38, § 87-3; Wis. Stat. § 134.43.

10. Video companies that violate the Video Privacy Protection Act of 1988 may be liable for actual damage awards of at least $2500, punitive damages, costs, and attorneys fees. 18 U.S.C. § 2710. They also may be subject to criminal penalties, civil fines, or damage awards under State video privacy laws. See, e.g., Mich. Comp. Laws § 445.1712; R.I. Gen. Laws § 11-18-32.

11. Where a financial institution discloses records or information in violation of the Right to Financial Privacy Act, the institution is liable to the customer for any actual

damages sustained, a $100 penalty, such punitive damages as the court may allow for willful or intentional violation, and court costs and attorney's fees. 12 U.S.C. § 3401, et seq.

12. Some states impose criminal and civil penalties for unauthorized disclosures of medical records. See, e.g., Cal. Civil Code § 56; Conn. Gen. Stat. § 52-146j; Mass. Gen. Laws ch. 111, § 70E; R.I. Gen. Laws § 5-37.3-9.

13. Employers that violate state statutes requiring them to provide their employees with access to personnel records are subject to civil and sometimes criminal penalties. See, e.g., Cal. Lab. Code § 1199; Mass. Gen. Laws ch. 149, § 52C; Ill. Stat. ch. 48, § 2012; Mich. Comp. Laws § 423.508.

14. The Fair Credit Reporting Act permits civil suits by individuals for violations of the Act by credit reporting agencies or parties who obtain consumer reports. Individuals may recover for actual damages suffered, as well as attorney's fees and court costs. Punitive damages may be awarded and criminal penalties imposed, for willful violations of the Act. Administrative enforcement is provided by the Federal Trade Commission or the particular Federal agency charged with responsibility for the various financial institutions subject to the Act. The agencies generally are empowered to declare actions to be in violation of the applicable statute, issue cease and desist orders, and impose statutory penalties for noncompliance with agency orders. 15 U.S.C. §§ 1681n-1681s.

15. The Fair Housing Statute subjects persons who unlawfully discriminate in housing to suit for injunctive relief, as well as actual and punitive damages, costs, and attorney's fees. Responsibility for administrative enforcement is vested in the Department of Housing and Urban Development. See 42 U.S.C. §§ 3610, 3612.

16. Employers who violate the Employee Retirement Income Security Act may be liable for statutory damage awards and subject to court-enforced injunctions ordering an end to illegal conduct. Suits may be brought by affected employees or the Treasury Department. The Department also is responsible for administrative enforcement of the statute. See 29 U.S.C. § 1132.

17. Employers using personal data in violation of the Equal Employment Opportunity Act may be compelled to cease their unlawful conduct and to undertake affirmative actions, such as the reinstatement of employees and payment of backpay. Primary responsibility for enforcing the Act rests with the Equal Employment Opportunity Commission and the U.S. Department

of Justice. Aggrieved individuals may sue only if the government does not sue or otherwise resolve the complaint. See 42 U.S.C. § 2000e-5.

18. In suits brought for violations of the Equal Credit Opportunity Act, successful plaintiffs may recover actual damages, punitive damages, attorney's fees and court costs. Individual or class action suits may be maintained for administrative, injunctive, or declaratory relief. The Federal agencies are given administrative enforcement responsibility. 15 U.S.C. § 1691c-1691e.

19. Under the Fair Credit Billing Act any creditor who fails to disclose required information is subject to a civil suit by individuals, with a minimum penalty of $100 and a maximum penalty not to exceed $1,000 on any individual credit transaction. The Act also imposes criminal liability on any person who knowingly and willfully gives false or inaccurate information, fails to disclose required information, or otherwise violates any requirement imposed by the Act. Any such person is subject to a fine of $5,000 and/or imprisonment for not more than one year. Administrative enforcement of the Act is accomplished by the Federal Trade Commission or the administration agencies charged with responsibility for the various financial institutions. 15 U.S.C. §§ 1607, 1611, 1640.

20. A debt collector who violates the Fair Debt Collection Practices Act is liable for any actual damages sustained, as well as any additional damages the court deems appropriate, not to exceed $1,000. A successful plaintiff also may recover court costs and attorney's fees. Administrative enforcement authority is lodged with the Federal Trade Commission, or with the Federal administrative agency charged with responsibility for a particular financial institution. 15 U.S.C. §§ 1692k, 16921.

21. Under the Electronic Funds Transfer Act, an individual who prevails in a civil action for violation of the Act may recover actual damages sustained, a penalty of $100 to $1,000, and attorney's fees and court costs. In limited situations a successful plaintiff may recover treble damages. Criminal penalties are also set out for deliberate violations of the Act. Finally, administrative enforcement responsibility is vested in the appropriate Federal agency. 15 U.S.C. §§ 1693m-1693o.

22. Enforcement of the Family Educational and Privacy Rights Act is achieved primarily through the right of students and their parents to inspect and challenge education records. Additionally, administrative enforcement of the Act is vested

in the Department of Education, and the Act provides for termination of Federal funds if an institution violates the Act and compliance cannot be secured voluntarily. 20 U.S.C. § 1232g.

23. Under the NAIC Model Act, the State insurance commissioner may issue cease and desist orders to prevent violations of the Act, as well as ordering payment of monetary penalties or suspension or revocation of an insurance company's or agent's license for knowing violations of the Act. Negligent violation of the Act's disclosure provisions will subject an insurance company or agent to liability for any actual damages sustained by an aggrieved plaintiff. Willful and knowing disclosure will result in liability for actual damages plus punitive damages up to three times the amount of actual damages. A successful plaintiff also may recover court costs and attorney's fees. Finally, any person who knowingly and willfully obtains information about an individual under false pretenses is subject to fine and/or imprisonment. See, e.g., Ill. Stat. ch. 73, §§ 1001-1024.

APPENDIX 3

MATRIX OF FEDERAL STATUTES ACCORDING TO
THE EC DIRECTIVE'S GENERAL PRINCIPLES

B. STATUTES AFFECTING PRIVATE SECTOR RECORDS

Federal Statute	Rights of Data Subjects		Obligations of Processors of Personal Information		Quality & Security of Information		Accountability & Sanctions	
	Notice or Consent	Access or Participation	Limitations on Access, Collection, or Use	Limitations on Disclosure	Accuracy	Unauthorized Access	Private Right of Action	Government Investigation or Prosecution
Cable Communications Policy Act	X	X	X	X			X	
Drug and Alcoholism Abuse Confidentiality Statutes			X	X				X
Electronic Communications Privacy Act	X	X	X	X		X	X	X
Electronic Funds Transfer Act	X	X	X				X	X
Employee Polygraph Protection Act	X		X	X			X	X

Federal Statute	Rights of Data Subjects		Obligations of Processors of Personal Information		Quality & Security of Information		Accountability & Sanctions	
	Notice or Consent	Access or Participation	Limitations on Access, Collection, or Use	Limitations on Disclosure	Accuracy	Unauthorized Access	Private Right of Action	Government Investigation or Prosecution
Employee Retirement Income Security Act		X					X	X
Equal Credit Opportunity Act	X		X				X	X
Equal Employment Opportunity Act			X				X	X
Fair Debt Collection Practices Act			X				X	X
Fair Credit Billing Act	X	X	X		X		X	X
Fair Credit Reporting Act	X	X	X	X	X	X	X	X
Family Educational Rights and Privacy Act	X	X	X	X				X

Federal Statute	Rights of Data Subjects		Obligations of Processors of Personal Information		Quality & Security of Information		Accountability & Sanctions	
	Notice or Consent	Access or Participation	Limitations on Access, Collection, or Use	Limitations on Disclosure	Accuracy	Unauthorized Access	Private Right of Action	Government Investigation or Prosecution
Fair Housing Statute			X				X	X
Health Research Data Statute				X				
Mail Privacy Statute			X				X	
Privacy Protection Act of 1980	X	X	X				X	
Right to Financial Privacy Act	X	X	X	X			X	
Tax Reform Act	X	X	X	X			X	X
Video Privacy Protection Act	X	X	X	X			X	
Wiretap Statutes	X		X	X			X	X

APPENDIX 4

LIST OF FEDERAL GOVERNMENT AGENCIES TO REPORT VIOLATIONS OF PRIVATE STATUTES

Persons aggrieved by violations of the federal statutes listed in this report can try suing in federal court. When appropriate, such violations also may be reported to the following federal agencies:

1. To report unauthorized disclosures of alcohol and drug abuse treatment records or unauthorized disclosures of personally identifiable alcohol and drug abuse data collected for research purposes, contact:

U.S. Public Health Service
Room 1741
Park Lane Building
5000-600 Fishers Lane
Rockville, MD 20857
(301) 443-2055

2. To report violations of the Fair Credit Reporting Act, Fair Credit Billing Act or Equal Credit Opportunity Act, contact:

Federal Trade Commission
Credit Practices Division
6th and Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-3175

3. To report violations of the Family Educational and Privacy Rights Act, contact:

U.S. Department of Education
Family Policy Compliance Office
Room 3017, FB-6
400 Maryland Avenue, S.W.
Washington, D.C. 20202-4605
(202) 401-2057

4. To report violations of the Employee Polygraph Protection Act, contact:

U.S. Department of Labor
ESA/Wage Hour
200 Constitution Avenue, N.W.
Washington, D.C. 20210
(202) 523-8305

5. To report violations of the Employee Retirement Income Security Act, contact:

U.S. Department of Labor
Pension and Welfare Benefits Administration
Division of Technical and Inquiries
Washington, D.C. 20210
(202) 523-8784

6. To report unauthorized disclosures of personally identifiable information collected by the U.S. Census Bureau, contact:

Deputy Chief Counsel
Bureau of the Census
Room 3077
Building 3
Washington, D.C. 20233
(301) 763-2818

7. To report employment discrimination on the basis of race, national origin, sex, etc., contact:

Equal Employment Opportunity Commission
1801 L Street, N.W.
Washington, D.C. 20507
(202) 663-4900

8. To report unauthorized publication of a communication by wire or radio, contact:

Federal Communications Commission
Enforcement Division
Common Carrier Bureau
2025 M Street, N.W.
Room 6206
Washington, D.C. 20554
(202) 632-4887

9. To report housing discrimination on the basis of race, national origin, sex, etc., contact:

Housing and Urban Development
Office of Fair Housing Enforcement
Section 3 Compliance
451 Seventh Street, SW
Room 5208
Washington, D.C. 20410
(202) 619-8041

10. To report unauthorized disclosures of federal income tax return information, contact: the local Internal Revenue Service's Problem Resolution Office in the District where the disclosure occurred.

11. To report violations of the Electronic Funds Transfer Act, contact:

Federal Reserve Board
Division of Consumer and Community Affairs
Washington, D.C. 20551
(202) 452-3693

12. To report unauthorized opening of mail, contact: the local Inspection Office of the U.S. Postal Service in the district in which the action occurred.

13. To report criminal violations of the Privacy Act, the Electronic Communications Privacy Act, federal computer crime statutes, and other federal statutes, contact: the local office of the Federal Bureau of Investigation in the district in which the act occurred.

PRIVACY PROTECTION LAW IN THE UNITED STATES

ROBERT ALDRICH

U.S. DEPARTMENT OF COMMERCE
Malcolm Baldrige, Secretary

Bernard J. Wunder, Jr., Assistant Secretary
for Communications and Information

MAY 1982

PRIVACY PROTECTION LAW IN THE UNITED STATES

INTRODUCTION

In September 1980, as a result of an effort by the world's industrialized nations to arrive at a framework for protecting international flows of personal information, the Organization for Economic Cooperation and Development (OECD) adopted "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (Guidelines).[1] The Guidelines recommend that, in connection with the collection, use, and disclosure of personal data, signatory countries adhere to eight principles, described as "minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties."[2] The Guidelines are applicable to both governmental and private records systems. The principles they incorporate, which have been variously described as standards of "data protection," "information privacy," and "fair information practice," have won increasing acceptance as basic rules for the management of personal data in the industrialized nations.

Paragraph 19 of the Guidelines recommends that in implementing the principles of privacy protection, "member countries establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data." In the United States, such implementation depends on legal requirements as well as self-regulation, or voluntary practice. The legal aspects of privacy protection -- the laws currently contributing to implementation of privacy principles in the United States -- are the subject of this report.

Privacy law in the United States is characterized by unusual diversity, as compared with the unitary schemes of regulation adopted by many countries of continental Europe. This report is not intended to be an exhaustive survey of U.S. laws. Instead, the purpose of the report is to illustrate the salient categories

of privacy law in the United States, and to explain some of the factors contributing to its great variety and its differential treatment of governmental and private information practices. Particularly for readers who are unfamiliar with the development of U.S. privacy law, an awareness of its varied roots and diverse functions may help in understanding how this complex body of law applies to specific privacy problems and to implementation of the Guidelines principles.

The main text of the report consists of three sections. In the first section, the diversity of U.S. privacy law is analyzed in terms of the law's sources, content, and means of enforcement. The second and third sections compare the law's treatment of privacy problems in the public and private sectors, respectively. Supplementing the main text are two appendices. Appendix I, a "Partial List of United States Privacy Laws," breaks down representative statutes, constitutional requirements, and common law principles covering the public and private sectors according to the groups of Guidelines principles to which they primarily apply. The vast majority of U.S. privacy laws were developed or enacted prior to the issuance of the Guidelines, and many of them incorporate a different conceptual framework from that of the Guidelines. Appendix I is intended to help in matching up U.S. privacy laws to relevant Guidelines principles.

Appendix II, "Descriptions of Selected Privacy Laws," discusses in greater detail the specific requirements of representative privacy laws. This appendix focuses on laws covering the private sector, because in this sphere the absence of an omnibus statute such as the Privacy Act of 1974 adds to the complexity of the task of identifying relevant laws. There is a considerable body of privacy law that regulates private record-keeping, but it is not all found in one place. Appendix II is intended as a guide to the main categories of private sector privacy law.

I. DIVERSITY OF THE LAW

Privacy law in the the United States is not limited to the Privacy Act of 1974: the law has sources in the Constitution and the common law as well as in legislation, and it includes statutes enacted by the States as well by the national legislature. The content of U.S. privacy law also varies considerably, depending on the type of record-keeping activity to which it applies. Finally, a number of different mechanisms are used to enforce these diverse legal requirements. In this section of the report, the variations in the sources, content, and methods of enforcement of U.S. privacy law are examined.

Diversity of Sources

The U.S. law of privacy is derived from a variety of sources, including the U.S. Constitution, the common law, and statutes and regulations at both Federal and State levels. This diversity reflects the historical process of accretion by which the law has developed, as well as the division of law-making authority, under the Federalist system, between the national government and the States.

The roots of privacy protection law in this country are found in the Constitution and the common law as well as in early statutes. Although the word "privacy" is nowhere mentioned in the Constitution, that document has historically played -- and continues to play -- a major part in protecting the values of privacy and liberty which are also the main concern of the OECD Guidelines. Among the fundamental safeguards established by the U.S. Constitution are guarantees of political and religious freedom, prohibitions against "unreasonable searches and seizures," and requirements for procedural fairness, or "due process of law." As the "supreme law of the land," such constitutional requirements can be repealed or superseded only by amendment of the Constitution itself, and they invalidate any conflicting statute. Moreover, the importance of the Constitution goes beyond its

specific legal application, as constitutional principles have strongly influenced the drafting of privacy legislation.

Privacy safeguards are also found in the "common law," a body of legal rules which originated in historical usages and customs and in the British laws given recognition by early U.S. courts, and which is continuously evolving through judicial interpretation. Common law may exist independently of any statute, though it is frequently modified or superseded by legislation. At the end of the nineteenth century, legal theorists proposed recognition of a general common law right to privacy, and since then the vast majority of States have recognized such a cause of action. In addition, the common law has provided basic privacy protections in such areas as defamation and breach of confidence.

Statutory law has played an increasingly important role in the development of U.S. privacy law. While serving to clarify and redefine the rights of individuals, new privacy statutes do not always supplant previous layers of statutory, constitutional, and common law. In banking, for example, the Right to Financial Privacy Act was not intended to replace the banker's common law duty of confidentiality, but to build upon it in order to address a new problem, the increasing collection of information from bank records by the Federal government. Similarly, enactment of the Privacy Act of 1974 left intact many earlier privacy-related statutes such as those covering census and tax data.

In addition to its long history of development, a second important diversifying influence on U.S. privacy law is the Federalist system of government in the United States. Although the concerns of the national government have expanded greatly over the last 50 years, there remains a strong presumption in our political culture that problems should be solved at the State level whenever it is practical to do so. A wide variety of privacy statutes have been enacted by the States, and responsibility for interpreting and applying common-law safeguards lies primarily with State courts.

The relationship between State and Federal legislative jurisdiction contributes substantially to the complexity of U.S. privacy laws. In some areas, Federal law has "preempted the field," invalidating all State laws pertaining to the subject in question. More frequently, State and Federal laws operate in tandem: when a Federal statute is enacted, Congress may explicitly or implicitly leave room for State laws to go further, and for State administrative authorities to supplement Federal enforcement.

In still other areas, Federal initiatives have been relatively insignificant, leaving the record-keeping activity to be regulated mainly by State law. The insurance industry, for example, is traditionally regulated by the States, as are the functions of State governments. In both these areas, nationwide organizations formed to promote harmony and uniformity among State laws have designed model privacy statutes. In the case of insurance, many companies that operate in more than one State have attempted to reduce their administrative costs by instituting company-wide compliance with the strictest applicable statute.

The broad dispersion of authority in the United States to make and interpret privacy law has assured that the issues are raised and debated at many levels, and at the same time has permitted essential experimentation in the development of solutions to privacy problems.

Diversity of Content

Diversity characterizes not only the sources, but also the type of protection offered by U.S. privacy laws. This diversity of content reflects the complexity of the modern idea of privacy, and the pragmatic approach that U.S. lawmakers have taken in applying a complex set of principles to varied record-keeping activities.

Until very recently, the term "privacy" in U.S. law referred primarily to the interests of individuals in being free from intrusion into their lives and in having

their personal affairs kept confidential by those to whom they were entrusted. In the United States, it was not until the early 1970s that privacy began to be defined in a broader sense, to include the interests of individuals in learning the contents of records about them and participating in setting conditions for their use. As a result, comprehensive privacy statutes such as the Fair Credit Reporting Act and the Privacy Act of 1974 address a number of concerns about institutional record-keeping practices which, though not necessarily ignored in the past, were not previously thought of as "privacy" problems.

The influence of innovative privacy theories on law-making processes has varied greatly. Although the Privacy Act directly incorporates a definition of information privacy or "fair information practice" that was published shortly before its enactment, other privacy laws do not adhere so rigorously to the new theoretical framework. Many of the laws implementing privacy principles have developed from older legal traditions -- for example, from traditional privacy concerns about limits on intrusive collection and unwarranted disclosure of information -- and consequently emphasize some aspects of modern privacy principles more heavily than others. Others were drafted in response to concerns which used to be distinguishable from "privacy" problems, but which today overlap with the territory covered by comprehensive privacy statutes. Addressing such issues as open government, due process, consumer protection, or equal opportunity, such statutes supplement and may even duplicate the requirements of explicitly labeled "privacy" laws. For example, the same set of government records may be subject to inspection by the individual under two different statutes: the Freedom of Information Act (an "open government" law) and the Privacy Act of 1974.

It is also significant that, in applying theories of privacy and related issues to specific record-keeping problems, U.S. lawmakers have on the whole taken a pragmatic approach. Many U.S. privacy safeguards have been tailored primarily to

the record-keeping function affected and to the nature of the perceived threat to an individual's interests, rather than to a general framework of record-keeping obligations. As a result, the legal rules for the application of privacy principles are not necessarily the same for all record-keeping activities. Privacy, no less than other issues, is subject to considerations of legislative economy -- that schemes of government regulation should not be needlessly established or extended. The absence of a single legal standard covering all record-keeping activity in the United States reflects a widely held belief that such a law would lead to far more government regulation than is desirable in this field.

In some sectors of record-keeping, comprehensive statutes -- such as the Privacy Act at the Federal level or the model insurance law in the States -- have been enacted to address most or all of the concerns covered by the Guidelines principles. However, such comprehensive legislation is supplemented by a great deal of more narrowly applicable privacy protection law, in the form of Constitutional and common law rules, and statutes targeted at specific record-keeping problems. In record-keeping industries where a comprehensive law such as the Privacy Act applies, the supplemental laws provide additional safeguards to cover record-keeping activities for which the general standards of a comprehensive statute may not be strong enough. In areas where a comprehensive statute has not been found necessary, more narrowly drawn statutes and rules serve to protect the interests of the individual which clearly require legal protection in that record-keeping context.

The diversity of content in U.S. privacy protection law may detract from its formal unity. However, it has also permitted flexibility of response by our courts and legislatures to privacy problems that vary widely in nature and importance.

Diversity of Enforcement

The third aspect of diversity in U.S. privacy laws is their means of enforcement. Privacy laws are enforced by individual lawsuits in court as well as by a variety of regulatory agencies at both the Federal and State levels. No single regulatory body has been created with a mandate to enforce all such laws. In part this is a direct consequence of the diversity in the law's sources and content. But there is another important factor explaining the decentralized enforcement structure of U.S. privacy law.

It is widely believed in the United States that the establishment of a central authority to administer an omnibus privacy law would set a dangerous precedent, by placing more and more privately-held personal data under the Federal government's supervision and control. In recommending against extension of the Privacy Act of 1974 to cover systems of records other than those held by the government, the U.S. Privacy Commission cited this concern: "Uniform and specific Federal requirements imposed on all private-sector record keepers and other governmental ones would inevitably require broad-based regulation, giving government an unprecedented role in channeling and monitoring flows of information throughout all of society."[3]

Primary authority for enforcing U.S. privacy laws is situated in the courts. The enforcement role of the courts, highly important in the U.S. legal system as a whole, is even more so in the case of privacy law because the courts have traditionally been perceived as the most reliable guardians of constitutional liberties. In addition to their usual powers to order compliance with the law, review administrative decisions, and award damages for violations, the courts have a special role in the protection of privacy: under the Fourth Amendment and related statutes such as the wiretapping laws and the Right to Financial Privacy Act, courts are often required to approve in advance the use of highly intrusive methods to collect personal information.

Administrative bodies also play a major role in enforcement of U.S. privacy protection law. A privacy statute is typically administered by the agencies that supervise the record-keeping industry to which the law applies. In the Federal government, oversight of the Privacy Act has been consolidated in the Office of Management and Budget with other functions related to the management of government records and "paperwork."

In addition to administrative enforcement and individual access to the courts, specific provisions of the laws themselves are designed to create incentives for compliance with privacy principles. The individual's right to inspect and challenge the contents of records, and the right to be notified of the purpose for which records are used and the reasons for decisions based on records are themselves an important means of preventing unwarranted collection, improper use, or inaccurate maintenance of personal data.

In the sections that follow, U.S. privacy law is described in greater detail. The laws applying to the government and to the private sector are treated in separate sections. Within each section, distinctions are drawn between comprehensive privacy statutes that embody the broad definition of privacy used in the OECD Guidelines, and "non-comprehensive" statutes or legal rules addressing specific privacy-related concerns such as confidentiality or due process.

II. PRIVACY LAW AND GOVERNMENT[4]

The centerpiece of U.S. privacy law affecting government record-keeping is the Privacy Act of 1974. Like the omnibus "data protection" laws enacted by many European nations, the Privacy Act is a response to the growing use of computers to handle personal data and to the tremendous expansion of the national government's role in the lives of individuals. Government programs such as welfare assistance,

social security, and medical and education assistance have required the government to amass huge quantities of personal information. At the same time, the sources of personal data accessible to the government have greatly expanded, with the growth of information-intensive services such as banking, credit, and insurance.

Unlike most of the U.S. privacy laws discussed in this paper, the Privacy Act incorporates in its entirety a theoretical framework that was developed explicitly to address the problems posed by computers and impersonal record-keeping institutions. From this theory of "fair information practice" -- the basic principles of which are also found in the OECD Guidelines and in many of Europe's data protection laws -- virtually all of the Privacy Act's requirements are directly derived.[5] Covering the vast majority of personal records systems maintained by the Federal government, the Privacy Act requires Federal agencies to publish annually a description of their personal records systems, and to notify individuals, when collecting information from them, of the purposes for which it will be used. Limits are placed on the type of information collected and the method of collection. Personal information may be disclosed, as a general rule, only with the individual's consent or for purposes announced in advance. The Act provides standards for accuracy and relevance as well as the security of personal data. And finally, individuals are entitled to inspect, copy, and challenge the contents of records about themselves.

However, the Privacy Act is by no means the sole source of privacy safeguards applying to government. Beginning with the Constitution, a large body of law has developed in the United States to regulate the information practices of government agencies, and to prevent them from using personal information in ways detrimental to basic liberties. The process of expanding and strengthening Constitutional guarantees of privacy and liberty in response to new technology and new uses of records has been a recurrent one in U.S. history. In earlier years, innovations such

as the telephone and telegraph, as well as the growth of information-intensive government functions such as the population census and tax collection, led to legislation and court decisions which aimed to prevent such changes from undermining the balance of power between citizens and government. These accumulated layers of law reflect deep-seated concerns that arbitrary actions of government pose the greatest threat to personal privacy and liberty.

Although the formal structure of the Privacy Act is new, the concerns underlying its enactment are very old by U.S. standards. Moreover, the background of Constitutional and legal theory from which the main principles of the Privacy Act are drawn includes not only traditional privacy rights, but also rights to non-discriminatory treatment and to procedural fairness, or "due process." These historical strands of which the theory of "fair information practice" is woven have continued to develop on their own in our legal system, creating independent networks of rights and obligations that overlap with the framework established by the Privacy Act.

Traditional Rights of Privacy

Many of the legal requirements supplementing the Privacy Act incorporate traditional ideas of privacy and confidentiality. Found in the Constitution as well as numerous statutes, such laws place additional and often quite strict limits on collection and disclosure of personal data by the government. The Fourth and Fifth Amendments to the Constitution, for example, have long provided a sphere of privacy around the individual that limits the methods used by the government to collect information about him or her. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. . . . " The scope of these protected areas is today defined as those in which the individual "has a reasonable expectation of

privacy," and includes technologically defined "zones of privacy" such as telephone transmissions, as well as the individual's person and property. As a general rule, the government cannot intrude into these areas to collect information without the individual's consent unless a "neutral and detached magistrate" has made a finding of "probable cause" that the evidence sought is relevant to an offense and is likely to be found in the specific places to be searched. The Fifth Amendment's privilege against self-incrimination provides a different sort of protection: it absolutely prohibits the government from compelling individuals themselves to provide information that would implicate them in criminal activity.

While demarcating a zone of privacy around the individual, these Constitutional requirements do not protect that zone completely: in the case of the Fourth Amendment, for example, persons and property may be searched upon a showing of "probable cause;" in the case of the Fifth Amendment, criminal investigations may be conducted and evidence obtained as long as the individual himself is not forced to divulge incriminating information. In effect, the Fourth and Fifth Amendments serve to assure "fair play" when the government intrudes on individual privacy.

As government has increased its involvement in areas of private life formerly considered solely the business of the individual, new safeguards have been enacted to protect privately held institutional records, which provide extensive documentation of an individual's personal affairs but which are not nearly as well protected by the Constitution as are an individual's private papers. For example, the Right to Financial Privacy Act of 1978 provides a mechanism regulating government access to bank records. Similarly, the Fair Credit Reporting Act of 1970 limits government access to information maintained by consumer reporting agencies, and requires a court order when information is acquired by the government for other than business purposes. Access by the Internal Revenue Service to certain records maintained by private recordkeepers is limited by the

Tax Reform Act of 1976, which like the Right to Financial Privacy Act includes a requirement for individuals to receive notice of and an opportunity to challenge disclosures.

In addition to placing limits on the government's collection of information from private sources, traditional privacy requirements also supplement the Privacy Act's safeguards for non-disclosure, or confidentiality, of personal information maintained by the government in the course of its business. Privacy rights of this sort have been established in part as an extension of similar rights in the private sector (e.g., because information was obtained from confidential sources such as medical records) and in part as a means of assuring the cooperation of the public in a data gathering effort such as the population census or tax administration. Under the Privacy Act, the principle of confidentiality was generalized to cover the vast majority of government records, and to require that such records be disclosed only for publicly announced purposes. However, many kinds of government records continue to be covered by separate confidentiality statutes, which often impose much stricter limits on disclosure than those of the Privacy Act.

Rights Against Discrimination

A second source of legal requirements supplementing the Privacy Act is the law relating to discrimination, which limits the use of "suspect" criteria in government decision-making. The Privacy Act and other comprehensive privacy statutes have borrowed less from this legal tradition than from others discussed in this paper. However, in view of the emphasis on non-discrimination in the OECD Guidelines,[6] any discussion of their implementation in the United States must refer to this separate and quite extensive body of law.

Perhaps the best-known example of laws against discrimination is the equal protection clause of the Fourteenth Amendment to the Constitution (applying

explicitly to the States, and to the Federal government by implication under the Fifth Amendment), which virtually bans the government from penalizing an individual because of race, color, or national origin, and which sharply limits discrimination on the basis of sex, illegitimacy, or alien status. Somewhat analogous limits on discrimination are established by the First Amendment to the Constitution, which restricts adverse treatment of individuals because of their political and religious beliefs and associations.

In addition to these Constitutional requirements, a number of statutes and regulations place more detailed restrictions on discrimination by the government. Some have added new categories to the list of "suspect" criteria, the use of which in decision-making processes is presumed to be unfair. Others, such as the the Privacy Act itself, broaden the scope of prohibited activity. Under the Privacy Act, the Federal government may not even maintain records about an individual's exercise of First Amendment rights, unless such records are "expressly authorized by statute" or "pertinent to and within the scope of an authorized law enforcement activity."

Rights to Procedural Fairness

A third source of rights supplementing those of the Privacy Act is the principle of "due process," which requires a fair opportunity for individuals to contest government action taken or proposed to be taken against them. Under the Fifth and Fourteenth Amendments to the Constitution, "due process" requirements originally applied to government action depriving the individual of liberty or property; as a result of expanding judicial interpretation of the due process clause and the enactment of statutes such as the Administrative Procedure Act, "due process" or procedural fairness (in the form of adequate notice and an opportunity to be heard in one's own defense) applies to a wide variety of government decisions

in which individuals have a stake. Before such decisions can become final, the individual is entitled, among other things, to scrutinize and challenge the factual record on which it is based.

Allusions to the principle of due process pervade the legislative history of the Privacy Act.[7] Although due process requirements have traditionally been triggered by specific actions or proposed actions of the government, those of the Privacy Act come into play whenever information is collected about an individual. One purpose of the Act's safeguards is to protect individuals when information about them is used to make informal, discretionary decisions of which they may be unaware. Specifically, individuals are entitled to learn why information is being collected about them and to inspect and dispute the contents of records. Another due process related objective of the Privacy Act is to assure that the less visible decision-making processes of government can be brought into the open. In addressing concerns about open government, the Privacy Act overlaps with other recently enacted Federal statutes such as the Freedom of Information Act and the Government-in-the-Sunshine Act.

III. PRIVACY LAW AND THE PRIVATE SECTOR[8]

Like the law applying to government, the privacy law applying to the private sector has developed from a number of related legal traditions. Unlike the public sector, however, private record-keeping activity is not covered by a single, comprehensive privacy statute. There are a number of reasons for this state of affairs, some of which were outlined by the Privacy Protection Study Commission in explicitly rejecting a proposal for such a statute: (1) the greater influence on the private sector of economic incentives that encourage voluntary compliance with privacy principles; (2) the difficulty of legislating a single standard for widely

varying record-keeping practices in the private sector, and (3) the danger of government control over private flows of information.[9]

In addition, the accumulation of personal data in the private sector is not widely perceived to be as inherently dangerous to fundamental liberties as in the case of government records. Although private sector organizations collect vast quantities of personal information about individuals, and although the use of such information can have serious consequences, the coercive powers of government are not available to such organizations. In the view of many, therefore, the mere presence of personal data in private files does not constitute as great a threat. Accordingly, private sector safeguards are more likely to be tailored to the type of records involved and the nature of the harm caused by their misuse.

The development of privacy law in the private sector, then, has been a selective process. In addition to the incremental evolution of common-law safeguards, much of the law applying to private record-keeping has accumulated through enactment of specifically targeted statutes, usually following a sharply focused legislative inquiry that identifies problems arising in a particular record-keeping relationship. Banks, employers, schools, and insurance companies each play a distinct role in the lives of individuals. Those roles largely determine the contents of personal records and how they are used. Accordingly, privacy protection requirements for the private sector vary significantly from one record-keeping relationship to another: what is needed to protect bank records may not be appropriate for insurance or employment records.

Some of the privacy law applying to the private sector does take the form of comprehensive statutes, similar to the Privacy Act of 1974, which apply a broad set of privacy principles to particular record-keeping industries. The Family Educational Rights and Privacy Act, the National Association of Insurance Commissioners' Insurance Information and Privacy Protection Model Act (enacted

in ten States since its approval by the Commissioners at the end of 1979), and the Fair Credit Reporting Act are examples of such comprehensive laws. The latter statute covers not only credit bureaus, but a variety of other information brokers that supply personal data about applicants for insurance, employment, government licenses, and other benefits. In order to protect individuals and allow them to interact with such organizations, with whom most people ordinarily have no direct contact, the Fair Credit Reporting Act sets standards for the collection, maintenance, and disclosure of personal data, and provides record-access and correction rights analogous to those of the Privacy Act. Comprehensive statutes of this sort are usually enforced through a combination of administrative supervision by existing regulatory authorities and private rights of action in court by the individuals themselves.

In contrast to comprehensive statutes, many of the laws applying to the private sector are not explicitly identified as privacy protection laws; nevertheless, they play a major role in furthering implementation of the Guidelines principles. Such requirements are found in diverse places, including consumer protection, equal opportunity, and confidentiality statutes; common-law tort principles such as defamation and intrusion; and express or implied contracts between banker and customer or doctor and patient. Many of these laws focus on particular kinds of record-keeping activity that pose an identifiable threat of harm to the individual. For example, the Fair Credit Billing Act, which establishes detailed requirements for the resolution of billing disputes in open-ended installment credit accounts, equips individuals to protect their privacy as well as financial interests in a specific type of situation for which strong procedural safeguards have been deemed necessary. Others provide a specific type of broadly applicable right --for example, against intrusive data collection methods or unfair discrimination.

Although the Constitution itself does not directly apply to private-sector record-keeping, the development of privacy law for that sector has been subject to the influence of Constitutional principles. As a result, there are many points of similarity between the legal requirements affecting government and private-sector record-keeping, and this paper uses the same categories in classifying them. In addition to the comprehensive statutes discussed above, the law of private record-keeping includes (1) traditional rights of privacy and confidentiality, as developed by the common law and supplemented by statute; (2) rights against discrimination by race and other suspect categories; and (3) rights to procedural fairness in institutional decision-making.

Traditional Rights of Privacy

The phrase "right to be let alone" was used by nineteenth-century American jurists to denote a variety of common-law principles then in force to protect various aspects of personal privacy.[10] Since that time, a number of common-law and statutory rights have been developed to protect the individual's interests in seclusion, the keeping of secrets, and reputation -- the interests which in ordinary language are associated with the word "privacy." The development of legal safeguards for these interests has a long and unsystematic history, and the description here will be confined to enumeration of the main branches of the law.

One branch of the common law of privacy is traceable to the laws of trespass, assault, and battery. The subcategory of the invasion-of-privacy tort known as "intrusion on physical solitude and seclusion" allows the collection of damages for invasion of one's person, property, and other "zones" of privacy, even though no physical damage has resulted.

A second branch of the law is rooted in the law of defamation, and protects against public disclosure of embarrassing private facts. Although the torts of defamation and public disclosure are related, it is important to distinguish the two. One obvious difference is that defamation involves statements that are untrue, while the privacy tort of public disclosure involves statements that, even though true, are inappropriate for publication. In addition, the level of publicity required to make defamation actionable is considerably lower than that required for a public disclosure action.

The third branch of common law privacy rights involves the keeping of secrets -- usually the confidences resulting from a professional or service relationship. This branch establishes the liability of physicians, attorneys, bankers, and others for unauthorized disclosure of confidential information entrusted to them. Common-law principles of confidentiality have frequently been codified in statutes -- in some cases merely stating the general principle, in others specifying authorized disclosures in some detail, including the inadmissibility of such information in court absent a waiver of its confidential status. Common law privacy safeguards and their statutory offspring are primarily enforced in the courts; however, in the case of professional confidences, either explicit or implicit enforcement powers are often vested in State licensing boards, and sometimes in Federal administrative bodies.

Rights Against Discrimination

A second major category of protections are those provided by equal opportunity statutes at the Federal and State level. Enacted to prevent discrimination with a serious impact on individual welfare, these statutes apply primarily to decisions on matters of economic importance to the individual. Examples at the Federal level include the Equal Credit Opportunity Act, the Equal Employment Opportunity Act,

and the Fair Housing statute. Administrative bodies have played a major role in the enforcement of equal opportunity laws, in part because proof of unfair discrimination often emerges only as a "pattern or practice" determined on the basis of statistical evidence covering many individual cases.

Rights to Procedural Fairness

A third category of private-sector law applies concepts of procedural fairness to private relationships. At the Federal level, such statutes apply mainly to the banking and credit sectors; however, there has been considerable legislative activity at the State level with respect to insurance, medical, and employment records. The main objective of such laws is to promote greater individual participation and, it is hoped, greater public confidence in private-sector decision-making processes, many of which are perceived as analogous to the operation of government bureaucracies. Examples of such laws at the Federal level are the Fair Credit Billing Act and the Electronic Funds Transfer Act, which attempt to promote fairness in the innovative but often impersonal relationships arising from the use of credit cards and electronic banking. Examples at the state level include statutes providing for individual rights of access to medical and employment records.

SUMMARY

The body of law implementing privacy protection principles in the United States has evolved in diverse, multi-jurisdictional layers, reflecting our pragmatic, pluralistic system as well as an inclination to avoid centralized authority over personal data. Much of the law is rooted in Constitutional restrictions on the power of government, and in the individual's common-law "right to be let alone."

In some areas, the source of protection is the Federal Congress and courts; however, the States have also acted to protect privacy in the many areas where they have traditionally asserted jurisdiction. As a result of the broad range of concerns covered by modern definitions of privacy, and the pragmatism that has informed the application of privacy principles, the content of privacy law varies widely for different kinds of record-keeping activity, with more comprehensive coverage of the government than of the private sector. The end result is a highly varied system of privacy law which nevertheless affords an extensive network of protections for the individual.

Footnotes

[1]Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: Organization for Economic Cooperation and Development, 1981)(hereafter Guidelines).

[2]Guidelines, Paragraph 6. The eight principles are as follows:

"Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

"Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

"Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

"Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.

"Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

"Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

"Participation Principle

13. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to

challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

"Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above."

Guidelines, Paragraphs 7-14.

[3]Privacy Protection Study Commission, Personal Privacy in an Information Society (Washington, D.C.: U.S. Government Printing Office, 1977)(hereafter Privacy Commission), p. 498. The Privacy Commission was established by the Privacy Act of 1974 to examine the effectiveness of existing privacy laws, review record-keeping practices in government and the private sector, and recommend what additional safeguards, if any, should be established.

[4]Citations to the laws discussed in this section can be found in Appendix I, Parts A through D.

[5]The concept of "fair information practice" was introduced in a study by the U.S. Department of Health, Education and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (Washington, D.C.: U.S. Government Printing Office, 1973).

[6]In addition to the general concerns about collection and use of personal data raised in Paragraphs 7 and 10 of the Guidelines, the question of unfair discrimination against data subjects on the basis of traits such as nationality, sex, race, creed, and trade union affiliation is specifically addressed by Paragraph 19.

[7]See Sen. Rept. 93-1183, 93d Cong., 2d Sess., pp. 14, 20, 49, reprinted in U.S. Senate, A Legislative History of the Privacy Act of 1974. A synthesis of "privacy" and "due process" was suggested by Alan Westin and Michael Baker in their study for the National Academy of Sciences, Databanks in a Free Society (New York: Quadrangle Press, 1972).

[8]Citations to the laws discussed in this section can be found in Appendix I, Parts E through H, and in Appendix II.

[9]Privacy Commission at 497-8.

[10]See, e.g., Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890); Cooley, Torts, 29 (2d ed. 1888)..

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4781

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
FEBRUARY 1992

4. TITLE AND SUBTITLE
Privacy Protection in the United States
A 1991 Survey of Laws and RegulationsAffecting Privacy in the Public and Private Sector Including a List of All Relevant Officials - Prepared by Ronald L. Plesser and Emilio W.

5. AUTHOR(S)
Cividanes of Piper and Marbury

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)
Reprinted by permission of the Piper & Marbury, Washington, DC 20036-2430.

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

This NISTIR, Privacy Protection in the United States, provides a survey of laws and regulations affecting privacy in both the public and private sector. It describes the fundamental principles of U.S. privacy protection policy, including developments in U.S. privacy law since 1982. Federal privacy guidelines and industry self-regulation are also discussed. Appendices include a glossary of U.S. privacy laws and a partial list of U.S. privacy laws.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

computer security, privacy, data protection, personal data, personal information

13. AVAILABILITY

X	UNLIMITED
	FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).
	ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.
X	ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
103

15. PRICE
A06

ELECTRONIC FORM